VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

BAKALÁŘSKÁ PRÁCE

Brno, 2020 Martin Bahna

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ
DEPARTMENT OF TELECOMMUNICATIONS

DETEKCE ANOMÁLIÍ V BEZDRÁTOVÝCH SÍTÍCH TYPU LORAWAN
DETECTION OF ANOMALIES IN LORAWAN TYPE OF WIRELESS NETWORKS

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — **Martin Bahna**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. Ondřej Pospíšil**
SUPERVISOR

BRNO 2020

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní program **Telekomunikační a informační systémy**

Ústav telekomunikací

Student: Martin Bahna ***ID:*** 197765
Ročník: 3 ***Akademický rok:*** 2019/20

NÁZEV TÉMATU:

Detekce anomálií v bezdrátových sítích typu LoRaWAN

POKYNY PRO VYPRACOVÁNÍ:

Student se v práci bude zabývat LPWAN protokolem LoRaWAN. Detailně se s protokolem i využívanou infrastrukturou seznámí a popíše bezpečnostní hrozby jednotlivých částí tohoto protokolu. V rámci praktické části si student vytvoří vlastní LoRaWAN síť, kde otestuje jednotlivé hrozby v rámci navržených scénářů (bezpečnostních incidentů) zahrnující identifikované hrozby. Z nasimulovaných bezpečnostních incidentů na základě logů a získaných informací navrhne, jak je možné detekovat jednotlivé hrozby na základě anomálií v rámci datového přenosu, komunikace, rádiových parametrů a dalších. Z dostatečného množství dat následně bude vytvořena statistika a graficky budou navržené metody detekce prezentovány.

DOPORUČENÁ LITERATURA:

[1] „LoRaWAN What is it?: A technical overview of LoRa and LoRaWAN.“ LoRa Alliance. 2015.

[2] MEKKI, Kais, et al. A comparative study of LPWAN technologies for large-scale IoT deployment. ICT express, 2019, 5.1: 1-7.

Termín zadání: 3.2.2020 ***Termín odevzdání:*** 8.6.2020

Vedoucí práce: Ing. Ondřej Pospíšil

prof. Ing. Jiří Mišurec, CSc.
předseda rady studijního programu

ABSTRAKT

Bakalárska práca je venovaná bezpečnosti v rámci bezdrôtovej siete LoRaWAN. V práci je všeobecne opísané IoT, jeho technológia, štandardy a komunikačné protokoly. Následne je opísaná technológia LPWAN, jej požiadavky a najpoužívanejšie protokoly používajúce túto technológiu. V práci je ďalej detailne opísaná technológia LoRaWAN s hlavným zameraním na jej bezpečnosť. Po bezpečnostnej analýze sú spomenuté najznámejšie útoky na túto technológiu spolu s možnými scenármi bezpečnostných incidentov. V rámci prakticej časti je opísaný postup zostrojenia vlastnej siete LoRaWAN, spolu s výberom a konfiguráciou komponentov. Následne je na sieť vykonaná dvojica útokov, realizovaných podľa daných scenárov. V poslednej časti je navrhnutý a opísaný spôsob detekcie týchto útokov.

KĽÚČOVÉ SLOVÁ

Bezpečnosť LoRaWAN, Detekcia anomálií v LoRaWAN, IoT, LoRaWAN, LPWAN

ABSTRACT

The present bachelor thesis deals with the LoRaWAN wireless network's security. First, IoT is defined in general, together with its technology, its standards and relevant communication protocols. Subsequently, the LPWAN technology is outlined, as well as its requirements and protocols that are most widely used with this technology. The thesis then describes the LoRaWAN technology further, with the focus maintained on its security. Following the security analysis, the most common attacks are mentioned, and possible security incident scenarios are recounted. The practical part of this thesis sheds some light on the process of personal construction of the LoRaWAN network, together with component selection and configuration. Two attacks are then performed on the network, carried out in accordance with the given scenarios. Lastly, a method of detecting these attacks is proposed and explained.

KEYWORDS

Anomaly detection in LoRaWAN, IoT, LoRaWAN, LoRaWAN security, LPWAN

BAHNA, Martin. *Detekce anomálií v bezdrátových sítích typu LoRaWAN*. Brno, 2020, 61 s. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací. Vedúci práce: Ing. Ondřej Pospíšil

VYHLÁSENIE

Vyhlasujem, že svoju bakalársku prácu na tému „Detekce anomálií v bezdrátových sítích typu LoRaWAN“ som vypracoval samostatne pod vedením vedúceho bakalárskej práce, s využitím odbornej literatúry a ďalších informačných zdrojov, ktoré sú všetky citované v práci a uvedené v zozname literatúry na konci práce.

Ako autor uvedenej bakalárskej práce ďalej vyhlasujem, že v súvislosti s vytvorením tejto bakalárskej práce som neporušil autorské práva tretích osôb, najmä som nezasiahol nedovoleným spôsobom do cudzích autorských práv osobnostných a/alebo majetkových a som si plne vedomý následkov porušenia ustanovenia § 11 a nasledujúcich autorského zákona Českej republiky č. 121/2000 Sb., o práve autorskom, o právach súvisiacich s právom autorským a o zmene niektorých zákonov (autorský zákon), v znení neskorších predpisov, vrátane možných trestnoprávnych dôsledkov vyplývajúcich z ustanovenia časti druhej, hlavy VI. diel 4 Trestného zákonníka Českej republiky č. 40/2009 Sb.

Brno ....

podpis autora

POĎAKOVANIE

Rád by som poďakoval vedúcemu bakalárskej práce pánovi Ing. Ondřejovi Pospíšilovi za odborné vedenie, konzultácie, trpezlivosť a podnetné návrhy k práci. Poďakovanie patrí aj rodičom za dlhodobú podporu a pomoc počas štúdia.

Obsah

Zoznam obrázkov

Zoznam tabuliek

Úvod

Bakalárska práca sa zaoberá LPWAN [1] (Low Power Wide Area Network) technológiou LoRaWAN [2] (Long Range WAN), s hlavným zameraním na bezpečnosť tejto technológie. LoRaWAN patrí medzi najpoužívanejšie LPWAN technológie, ktoré sú neoddelitelnou súčasťou IoT [3] (Internet of Things) najmä vďaka ich vysokému bezdrôtovému dosahu a minimálnemu odberu elektrickej energie.

V prvej kapitole je všeobecne popísané čo rozumieme pod pojmom internet vecí, jeho využitie v praxi, výhody a nevýhody a samotná technológia IoT. Sú tu tiež priblížené štandardy a komunikačné protokoly používané v IoT.

Druhá kapitola je venovaná technológii LPWAN, jej možné širokosiahle využitie a požiadavky na technológiu. Ďalej sú bližšie popísané najpoužívanejšie protokoly využívajúce túto technológiu.

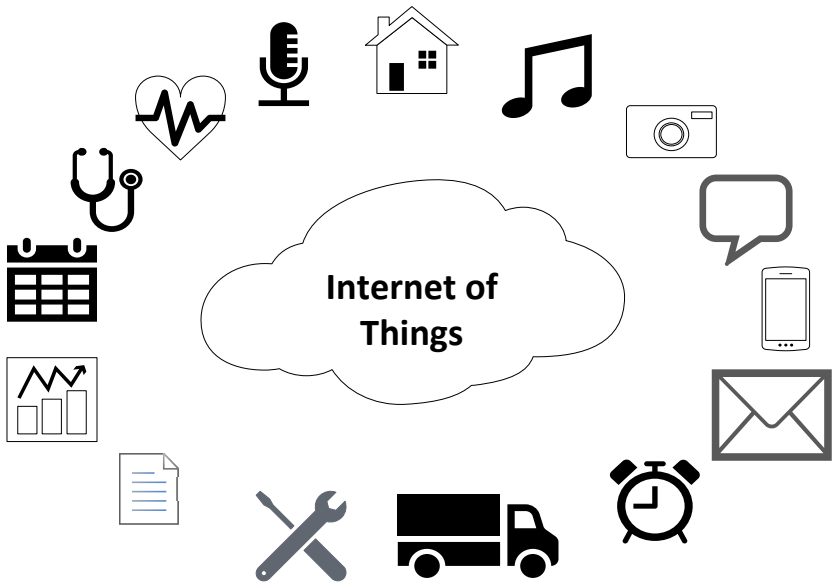
Tretia kapitola sa zaoberá už konkrétne protokolom LoRaWAN. Protokol je detailne popísaný, od jeho štruktúry, cez požiadavky, jeho verzie a sieťovú architektúru až po bezpečnostné riešenia. Práca sa zaoberá práve bezpečnosťou tohto protokolu, preto mu je táto kapitola podrobne venovaná [4].

Ďalšia kapitola je venovaná najznámejším bezpečnostným hrozbám, ktorým siete LoRaWAN čelia v praxi. Po priblížení jednotlivých útokov sú navrhnuté dva kompletné scenáre bezpečnostných incidentov [5].

V záverečnej kapitole je popísaná praktická časť bakalárskej práce. Je tu opísané zostrojenie vlastnej siete LoRaWAN, kde sú popísané jednotlivé vybrané komponenty a ich konfigurácia. Po zostrojení siete boli uskutočnené bezpečnostné incidenty podľa vypísaných scenárov. Nakoniec je uvedená možnosť a realizácia detekcie týchto incidentov na základe anomálií v sieti.

1 Internet of Things

Internet of Things (IoT), alebo v preklade Internet vecí je pojem, s ktorým sa v bežnom živote stretávame čoraz viac. Jedná sa o koncept prepojenia bežných zariadení, ktoré ľudia používajú na dennej báze ako sú napríklad práčky, chladničky, ale aj obyčajné elektrické zásuvky ai. viď obr. 1.1. V podstate ide o komunikáciu človeka s daným prístrojom, kde sa predávajú informácie ako napríklad kedy má práčka začať prať, alebo kedy sa má vypnúť vyhrievacie teleso pripojené do elektrickej zásuvky a pod. Táto komunikácia je založená na rôznych komunikačných protokoloch, ktoré umožňujú nielen komunikáciu medzi človekom a daným prístrojom ale aj medzi prístrojmi navzájom. Predané informácie sa ďalej vyhodnocujú, spracovávajú až sa nakoniec dostaneme k finálnemu výsledku kde prístroj vo väčšine prípadov spraví to, čo od neho očakávame. Celý princíp Internetu vecí je založený na uľahčení bežného života obyčajných ľudí, ale aj na zefektívnenie výroby v priemysle a hospodárstve.



Obr. 1.1: Internet of Things [6].

Hlavné výhody IoT:

- Možnosť prístupu k informáciám odkiaľkoľvek v akomkoľvek čase z akéhokoľvek zariadenia.
- Zdokonalená komunikácia medzi pripojenými elektronickými zariadeniami.
- Prenášanie dátových paketov cez sieť šetrí čas aj náklady [3].
- Automatizácia pomáha rozvoju kvality a redukuje potrebu zásahu ľudskej zložky.

Niektoré nevýhody IoT:

- Rastúcim počtom pripojených zariadení rastie aj počet prenášaných dát medzi zariadeniami čím sa zvyšuje riziko potencionálnej krádeže citlivých informácií hackermi.
- Veľké podniky sa stretávajú s masívnymi počtami, niekedy miliónmi, IoT zariadení čo spôsobuje zbieranie a spracovávanie informácií zo všetkých týchto zariadení veľmi komplikovaným [3].
- Ak nastane nejaká systémová chyba (bug), je veľmi pravdepodobné, že to ovplyvní všetky zariadenia pripojené do siete.
- Neexistuje žiadny medzinárodný štandard kompatibility pre IoT, preto sa môžu vyskytnúť komplikácie pri komunikácii zariadení od odlišných výrobcov.

1.1 IoT technológia

Zariadenie väčšinou pozostáva z procesoru, senzoru, ktorý zbiera informácie a komunikačného modulu, ktorý zozbierané informácie posiela ďalej buď bráne (gateway) prípadne inému koncovému zariadeniu, ktoré zbiera dané údaje na poslanie ďalej na cloud či server, prípadne ich lokálne spracováva, alebo môžu byť dáta poslané aj na iné zariadenie IoT kde sa tieto dáta porovnávajú navzájom a následne je vykonaná ďalšia operácia [3]. Celá komunikácia funguje bez zásahu človeka, aj keď človek môže danému prístroju zadávať inštrukcie či pristúpiť k zozbieraným informáciám.

1.1.1 Štandardy a komunikačné protokoly

Pre komunikáciu v IoT existuje veľké množstvo protokolov, preto budú rozdelené do niekoľkých kategórií [7]:

Infraštruktúrne protokoly

- **IPv6 (Internet protokol verzia 6)** je protokol pracujúci na Sieťovej vrstve slúžiaci na prepájanie paketov v sieťach a poskytuje end-to-end posielanie datagramov cez niekoľko IP sietí.
- **6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks)** je open štandard umožňujúci akúkoľvek nízkoenergetickú komunikáciu do internetu. Pracuje iba na 2,4 GHz frekvencii s prenosovou rýchlosťou 250 kb za sekundu.

- **UDP (User Datagram Protocol)** je jednoduchý OSI transportný protokol pre sieťové aplikácie typu klient/server založený na Internetovom protokole (IP). UDP je hlavná alternatíva k TCP a jeden z najstarších existujúcich protokolov (používa sa od roku 1980). UDP je prioritne používaný v aplikáciách pre komunikáciu v reálnom čase.
- **uIP** je open source TCP/IP zásobník, ktorý je možné použiť v malých 8 a 16-bitových mikrokontroléroch.
- **DTLS (Datagram Transport Layer)** poskytuje bezpečnú komunikáciu pre datagramové protokoly. Tento protokol umožňuje aplikáciám typu klient/server komunikovať spôsobom akým boli navrhnuté bez hrozby odpočúvania, či falšovania správ. Založený je na TLS (Transport Layer Security) protokole a poskytuje ekvivalentné bezpečnostné záruky.
- **TSMP (Time Synchronized Mesh Protocol)** je komunikačný protokol vytvorený pre samo-organizačné siete bezdrôtových zariadení. TSMP zariadenia sú medzi sebou synchronizované a komunikujú v časových úsekoch.

Dátové protokoly

- **MQTT (Message Queuing Telemetry Transport)** je protokol, ktorý umožňuje jednoduchý spôsob publikovania správ. Používa sa na spojenia väčších vzdialeností kde sa používajú malé kódy a malá šírka pásma.
- **CoAP (Constrained Application Protocol** je protokol pracujúci na aplikačnej vrstve, ktorý pracuje na zariadeniach v sieti s obmedzenými zdrojmi. Bol dizajnovaný na jednoduchý preklad do HTTP pre zjednodušenú operáciu s webom, kým spolupracuje s inými špeciálnymi požiadavkami ako multicastová podpora, nízka záťaž a jednoduchosť.
- **XMPP (Extensible Messaging and Presence Protocol)** je open source technológia pre komunikáciu v reálnom čase, ktorá obsluhuje širokú škálu aplikácií vrátane rýchlych správ, kontrolovania prítomnosti, audio-video hovorov resp. generalizovaného smerovania XML dát.
- **LWM2M (Lightweight M2M)** je systémový štandard Open Mobile Alliance. Zaisťuje komunikáciu na aplikačnej vrsve medzi klientom a serverom. Slúži na správu senzorov, prenos dát zo siete k zariadeniu a je rozšírený tak, aby vyhovoval požiadavkám väčšiny aplikácií.
- **SSI (Simple Sensor Interface)** je jednoduchý komunikačný protokol dizajnovaný na dátový prenos medzi počítačom a inteligentným senzorom.
- **Websocket** definuje full-duplex single socket konektivitu na prenášanie správ medzi klientom a serverom. Tento štandard zjednodušuje obojsmernú webovú komunikáciu a jej ovládanie.

Komunikačné protokoly

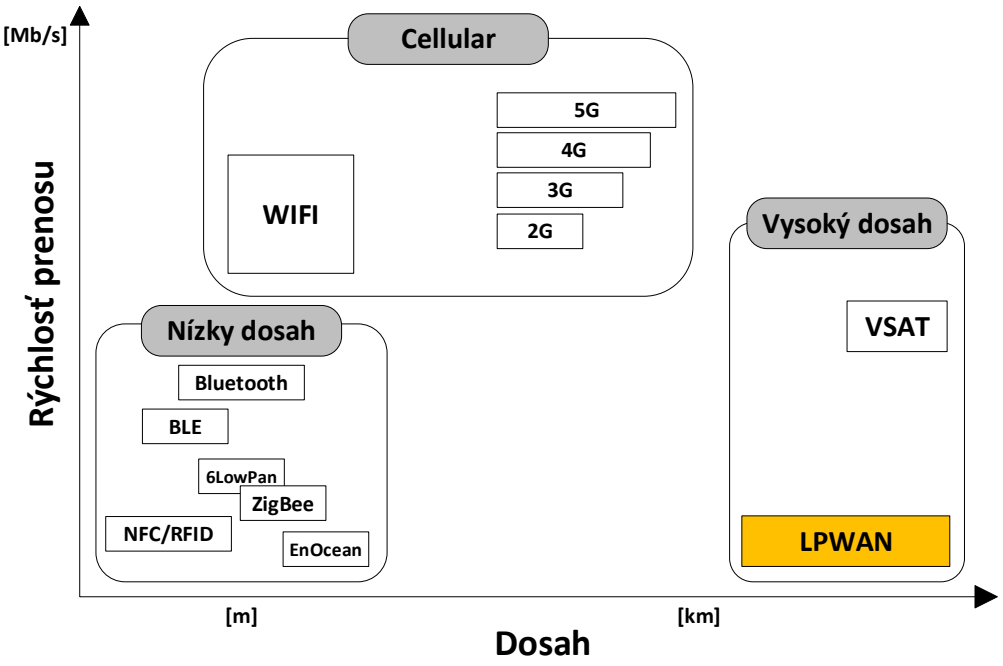
- **Ethernet** je štandard IEEE 802.3 pre drôtový prenos po krútenej dvojlinke a optických vláknach, ktoré dosahujú rýchlosť až stovky Gb za sekundu.
- **NFC** je založený na štandarde ISO/IEC 18092:2004, používajúc zariadenia na frekvencii 13,56 MHz. Rýchlosť prenosu dosahuje až 424 kb za sekundu s dosahom niekoľko metrov.
- **Bluetooth** pracuje v 2,4 GHz ISM pásme a používa frekvenčné preskakovanie. Rýchlosť prenosu dosahuje 3 Mb za sekundu s maximálnym dosahom 100 metrov. Každá aplikačný typ, ktorý používa Bluetooth má svoj vlastný profil.
- **ZigBee** je protokol pod štandardom 802.15.4 pracujúci na frekvencii 2,4 GHz s prenosovou rýchlosťou 250 kb za sekundu. Maximálny počet koncových zariadení v sieti je 1024 s maximálnym dosahom 200 metrov. ZigBee vie tiež implementovať 128 bitové AES šifrovanie.
- **EnOcean** je technológia, ktorá pracuje na frekvenciách 868 MHz pre Európu a 315 MHz pre Severnú Ameriku. Maximálny dosah je 30 metrov v budovách a 300 metrov vo voľnom prostredí.
- **Wi-Fi** je štandard IEEE 802.11 pre bezdrôtovú komunikáciu pracujúci na frekvenciách 2,4 GHz a 5 GHz. Dokáže komunikovač na vzdialenosť stoviek metrov a prenosová rýchlosť sa odvíja od konkrétneho typu 802.11.
- **Cellular** technológie GPRS, 2G, 3G a 4G.
- **LPWAN (Low Power Wide Area Network)** je spôsob komunikácie na veľké vzdialenosti s nízkou spotrebou energie. Používa protokoly ako Sigfox, NB-IoT, LoRaWAN, Weightless ai.

Bezpečnosť

- **OTrP (Open Trust Protocol)** je protokol slúžiaci na inštaláciu, update a mazanie aplikácií, a na ovládanie bezpečnostnej konfigurácie v TEE (Trusted Execution Enviroment).
- **X.509** je štandard pre infraštruktúru verejného kľúča na upravovanie digitálnych certifikátov a šifrovanie verejného kľúča. Kľúčová časť TLS (Transport Layer Security) protokolu používaná na zabezpečenie webu a emailovej komunikácie.

2 Low Power Wide Area Network

V dnešnej dobe rastie dopyt po IoT technológiách obrovským tempom vďaka veľkému spektru využiteľnosti v rôznych aplikáciách ako napr. bezpečnosť, poľnohospodárstvo, inteligentné mestá či inteligentné domácnosti. Tieto aplikácie majú špecifické požiadavky ako napríklad komunikácia na veľkú vzdialenosť, malé množstvo prenášaných dát, nízka spotreba energie a cenová dostupnosť. V praxi sa stretávame s podobnými technológiami ako je Bluetooth, ktorý však nespĺňa požiadavku pre komunikáciu a veľké vzdialenosti, alebo mobilná komunikácia (2G, 3G a 4G), ktorá síce dokáže pokryť rozľahlé územie no naopak má vysokú spotrebu elektrickej energie zo zariadení. Preto bola vyvinutá nová bezdrôtová technológia, ktora spĺňa všetky vyššie uvedené požiadavky a to je LPWAN (Low Power Wide Area Network). Rozdelenie týchto, ale aj iných technológií môžme tiež vidieť na obr. 2.1.



Obr. 2.1: Porovnanie technológie LPWAN s inými bezdrôtovými technológiami [8].

2.1 Požiadavky

LPWAN technológia je populárna hlavne v priemyselných a výskumných oblastiach vďaka nízkej spotrebe energie, veľkému pokrytiu a nízkym komunikačným nákladom. Medzi najzákladnejšie požiadavky patrí pokrytie veľkého územia, v praxi až do 10–40 km v neosídlených oblastiach a 1–5 km v osídlených oblastiach. Ďalšou základnou požiadavkou je vysoká energetická účinnosť, rádovo sa jedná o 10 + rokov

výdrže batérie [1]. Treťou hlavnou požiadavkou je cenová dostupnosť kde rádiový chipset stojí menej ako 2 € a prevádzkové náklady sa pohybujú okolo 1 € na rok na zariadenie. Vďaka týmto aspektom je LPWAN technológia priam ideálna pre použitie v IoT aplikáciách, ktoré potrebujú posielať malé množstvo dát na veľkú vzdialenosť. Vzniklo množstvo LPWAN technológií v licencovanej aj nelicencovanej podobe, popredné a najpoužívanejšie sa však stali Sigfox, LoRa a NB-IoT [1], ktoré zahŕňajú mnoho technických rozdielov a preto budú popísané bližšie.

2.2 Rozdiely LPWAN technológií

Technológie Sigfox, LoRa a NB-IoT sa líšia v mnohých technických aspektoch ako je popísané v tab. 2.1. Najhlavnejšie rozdiely spočívajú v použitej modulácii, prenosovej rýchlosti, veľkosti payloadu[1] a spôsobe overovania a šifrovania komunikácie.

Tab. 2.1: Prehľad LPWAN technológií: Sigfox LoRa a NB-IoT [1].

	Sigfox	**LoRaWAN**	**NB-IoT**
Modulácia	BPSK	CSS	QPSK
Frekvencia	Nelicencované ISM pásma (868 MHz v Európe, 915 MHz v Severnej Amerike, 433 MHz v Ázii)	Nelicencované ISM pásma (868 MHz v Európe, 915 MHz v Severnej Amerike, 433 MHz v Ázii)	Licencované LTE pásma
Šírka pásma	100 Hz	250 kHz a 125 kHz	200 kHz
Maximálna prenosová rýchlosť	100 bps	50 kbps	200 kbps
Obojsmerný prenos	Limitovaný / Polovičný duplex	Áno / Polovičný duplex	Áno / Polovičný duplex
Maximum správ za deň	140 poslaných, 4 prijaté	Nelimitované	Nelimitované
Maximálny payload	12 bajtov (UpLink), 8 bajtov (DownLink)	243 bajtov	1600 bajtov
Dosah	10 km (osídlené oblasti), 40 km (neosídlené oblasti)	5 km (osídlené oblasti), 20 km (neosídlené oblasti)	1 km (osídlené oblasti), 10 km (neosídlené oblasti)
Overovanie a šifrovanie	Nepodporované	Áno (AES 128b)	Áno (LTE šifrovanie)
Adaptívna rýchlosť prenosu dát	Nie	Áno	Áno

2.2.1 Sigfox

Sigfox je LPWAN sieťový operátor ktorý ponúka end-to-end IoT riešenie konektivity skrz patentované technológie. Sigfox používa vlastné stanice, pripojené k back-end serverom. Koncové zariadenia pripojené k týmto staniciam používajú moduláciu binárneho fázového posunu (BPSK) v ultra úzkopásmovom (100 Hz) sub-GHZ ISM pásmovom nosiči. Sigfox používa nelicencované ISM pásma napr. 868 MHz v Európe, 915 MHz v Severnej Amerike a 433 MHz v Ázii. Použitím ultra úzkopásmového prenosu, Sigfox dokáže efektívne využiť šírku pásma a má veľmi nízku úroveň šumu, čo

[1]Payload je časť prenášaného obsahu, ktorá obsahuje užitočné dáta pre používateľa.

spôsobuje nízky odber elektrickej energie, vysokú citlivosť prijímača a nízkorozpočtový dizajn antény na úkor maximálnej prenosovej rýchlosti iba 100 bitov za sekundu. Sigfox na začiatku podporoval iba uplinkovú komunikáciu, ale neskôr začal podporovať komunikáciu obojsmernú. Downlinková komunikácia, teda dáta posielané zo stanice do koncových zariadení, môžu byť poslané iba za uplinkovou komunikáciou. Počet správ odoslaných koncovým zariadením do stanice je limitovaný na 140 správ za deň. Maximálny payload pre každú odoslanú správu môže byť 12 bajtov. Avšak správy prijaté koncovým zariadením zo stanice sú limitované na štyri denne, čo znamená, že potvrdzovanie správ nieje podporované. Maximálny payload pre každú prijatú správu je 8 bajtov. Bez adekvátnej podpory potvrdzovania je spoľahlivosť uplinkovej komunikácie zabezpečená pomocou časovej a frekvenčnej diverzity ako aj duplikovaným posielaním správ. Každá správa z koncového zariadenia je posielaná niekoľko krát (štandardne 3 krát) po odlišných frekvenciách. Pre tieto účely je napríklad v Európe používané frekvenčné pásmo medzi 868,180 MHz a 868,220 MHz rozdelené na 400 ortogonálnych 100 Hz kanálov (medzi nimi je 40 kanálov vyhradených a nepoužívajú sa). Vďaka tomu, že stanica dokáže prijímať naraz správy na všetkých frekveciách, môže koncové zariadenie vyberať náhodné frekvencie na prenos dát [1].

2.2.2 NB-IoT

NB-IoT je Narrow Band IoT technológia špecifikovaná vo Vydaní 13 3GPP v Júni 2016. NB-IoT dokáže koexistovať s GSM (global system for mobile communications) a LTE (long-term evolution) pod licencovanými frekvenčnými pásmami (napr. 700 MHz, 800 MHz a 900 MHz). NB-IoT využíva frekvenčné pásmo šírky 200 kHz, čo zodpovedá jednému bloku GSM a LTE prenosu. S touto šírkou pásma je možné pracovať s prevádzkovými režimami:

- **Samostatná operácia:** možným scenárom je využitie v súčasnosti používaných GSM frekvenčných pásiem.
- **Operácia v ochrannom pásme:** využitie nepoužitých blokov LTE chráneného frekvenčného pásma.
- **Pásmová operácia:** využitie blokov vrámci LTE frekvenčného pásma.

V skutočnosti NB-IoT redukuje funkcionality LTE protokolu na minimum a zlepšuje ich podľa potrieb IoT aplikácií. NB-IoT teda možno považovať za nový protokol, ktorý je postavený na LTE infraštruktúre. Tento protokol umožňuje pripojenie až do 100 000 koncových zariadení na bunku s potenciálom na zväčšenie kapacity pridaním viacerých NB-IoT nosičov. Používa single-carrier FDMA (frequency division multiple access) pre uplink a ortogonálny FDMA (OFDMA) pre downlink a zapája aj QPSK (quadrature phase-shift keying) moduláciu. Prenosová rýchlosť je limito-

vaná na 200 kilobitov za sekundu pre downlink a 20 kilobitov za sekundu pre uplink. Maximálny payload je pre každú správu 1600 bajtov. NB-IoT technológia dokáže zabezpečiť až 10 rokov výdrže batérie pri vysielaní priemerne 200 bajtov denne [1].

2.2.3 LoRaWAN

LoRa je modulácia pracujúca na fyzickej vrstve, ktorá moduluje signál v sub-GHZ ISM pásme použitím proprietárnej techniky rozšíreného spektra. Tak ako Sigfox aj LoRa využíva nelicencované ISM frekvenčné pásma 868 MHz v Európe, 915 MHz v Severnej Amerike a 433 MHz v Ázii. Obojsmerná komunikácia funguje pomocou CSS (Chirp Spread Spectrum[2]) modulácie, ktorá šíri úzkopásmový signál cez kanály s väčšou šírkou pásma. Výsledný signál má nízku úroveň šumu, čo zabezpečuje, že má vyššiu odolnosť voči rušeniu a tým je ťažké signál detekovať a narušiť.

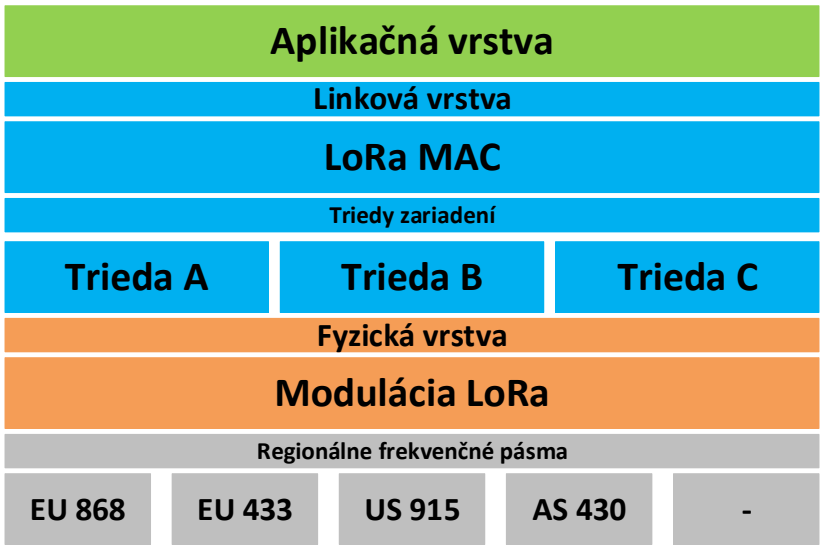
LoRa využíva šesť faktorov šírenia (spreading factors) od SF7 do SF12 na prispôsobenie rýchlosti prenosu údajov. Čím vyšší je faktor šírenia, tým väčší je dosah, avšak na úkor prenosovej rýchlosti. Prenosová rýchlosť sa pohybuje medzi 300 bitov až 50 kilobitov za sekundu v závislosti na faktore šírenia a šírke pásma kanálu. Správy posielané použitím rôznych faktorov šírenia môžu byť prijaté LoRaWAN stanicami súčasne. Maximálny payload pre každú správu je 243 bajtov. Komunikačný protokol LoRaWAN, založený na modulácii LoRa, bol štandardizovaný spoločnosťou LoRa-Alliance. Použitím LoRaWAN protokolu je každá správa vyslaná koncovým zariadením prijatá každou stanicou v dosahu. Týmto spôsobom si protokol LoRaWAN zaisťuje vysoký pomer úspešne doručených správ. Je to však na úkor vyššieho počtu staníc v dosahu, čo môže spôsobiť vyššiu cenu za zavedenie siete. Výsledné duplicitné záznamy sa filtrujú v backendovom systéme (server), ktorý obsahuje potrebnú inteligenciu na zaistenie bezpečnosti, posielanie potvrdzovaní na koncové zariadenia a odosielanie správ na zodpovedný aplikačný server [1].

Keďže je táto práca venovaná práve technológii LoRaWAN, bude okrem tohto stručného zhrnutia technológii venovaná ďalšia kapitola kde bude LoRaWAN popísaná bližšie.

[2]Technika rozšíreného frekvenčného spektra, ktorá používa širokopásmové lineárne modulované "cvrlikajúce" impulzy na šifrovanie informácie [9].

3 Long Range WAN

Ako bolo spomenuté už v predchádzajúcej kapitole, technológia LoRaWAN je open standard od organizácie LoRa Alliance. LoRaWAN je technológia použiteľná na veľké vzdialenosti s nízkou rýchlosťou prenosu dát a má nízke energetické požiadavky. Na obr. 3.1 sú znázornené jednotlivé vrstvy LoRaWAN technológie.



Obr. 3.1: Rozdelenie vrstiev v LoRaWAN [10].

3.1 Fyzická vrstva LoRa modulácie

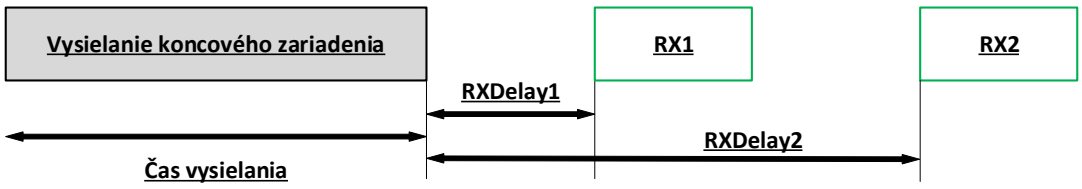
LoRa pracuje na fyzickej vrstve využívajúc bezdrôtovú moduláciu pre vytvorenie linky na komunikáciu s vysokým dosahom. Mnohé staršie bezdrôtové systémy používajú moduláciu FSK (frequency shifting keying) ako fyzickú vrstvu, pretože je to efektívne pre nízku spotrebu energie. LoRa je založená na CSS (Chirp Spread Spectrum) modulácii, ktorá zabezpečuje rovnako nízku spotrebu ako FSK modulácia, ale podstatne zvyšuje komunikačný dosah. CSS modulácia sa pred komerčným využívaním v LoRa modulácii používala aj pre armádne a vesmírne účely vďaka veľkému dosahu.

Výhodou modulácie LoRa je jej schopnosť pokryť veľké územia. Jeden gateway (brána), alebo stanica, dokáže pokryť celé mesto, prípadne rozlohu o veľkosti stoviek kilometrov štvorcových. Dosah veľmi závisí od prostredia a prekážok v danej lokácii, ale LoRa modulácia má link budget väčší ako iné štandardizované komunikačné technológie. Link budget, väčšinou vyjadrený v decibeloch (dB), je hlavný faktor v určení dosahu v danom prostredí.

3.2 Linková vrstva

Zatiaľ čo modulácia LoRa na fyzickej vrstve zabezpečuje komunikačnú linku na veľkú vzdialenosť, LoRaWAN definuje komunikačný protokol a systémovú architektúru siete. Protokol a sieťová architektúra majú najväčší vplyv v určovaní životnosti batérie uzla, kapacity siete, QoS (Quality of Service), bezpečnosti a rôznych aplikácií poskytované sieťou. Technológia LoRaWAN využíva zariadenia rozdelené do troch tried. Práve tieto triedy definujú vyššie spomenuté parametre jednotlivých zariadení [2].

- **Obojsmerné koncové zariadenia (trieda A):** koncové zariadenia triedy A podporujú obojsmernú komunikáciu, kde je každá uplinková komunikácia (správy zaslané zariadením do stanice) nasledovaná dvomi krátkymi downlinkovými oknami ako je znázornené na obr. 3.2. Skupina správ naplánovaná koncovým zariadením je založená na komunikačných potrebách koncového zariadenia s malou odchýlkou založenou a náhodnom čase (používa sa protokol ALOHA). Táto operácia triedy A je energeticky najúspornejší systém pre aplikácie, ktorý potrebuje len krátku downlinkovú komunikáciu, po tom ako koncové zariadenie pošle uplinkovú správu stanici. Downlinková komunikácia stanice v inom čase musí teda vyčkať kým nebude prijatá uplinková správa z koncového zariadenia.
- **Obojsmerné koncové zariadenia s plánovaným prijímaním (trieda B):** oproti triede A, ktorá prijíma správy náhodne, zariadenia triedy B očakávajú správy zo staníc v určenom čase. Aby koncové zariadenie začalo prijímať v stanovenom čase, prijme časovo-synchronizačný signál zo stanice. Podľa toho sieťový server rozpozná, že koncové zariadenie je pripravné na prijatie správy. Zariadenie tejto triedy sa nazýva aj Beacon (v preklade maják).
- **Obojsmerné koncové zariadenia s nepretržitou dobou prijímania (trieda C):** koncové zariadenia triedy C sú takmer vždy pripravené na prijímanie správ od stanice až na čas kedy samy vysielajú na úkor nadmernej spotreby elektrickej energie.



Obr. 3.2: Komunikácia zariadenia a stanice LoRaWAN triedy A [1].

3.3 Parametre

Tak ako každá technológia v IoT, tak aj LoRaWAN je definovaná niekoľkými rôznymi parametrami.

3.3.1 Kapacita siete

Aby mala sieťová architektúra v tvare hviezdy čo najvyššiu účinnosť, musí mať brána vysokú kapacitu, resp. musí byť schopná prijať veľké množstvo správ z jednotlivých uzlov. Vysoká kapacita v LoRaWAN sieti je dosiahnutá využitím adaptívnej prenosovej rýchlosti a použitím multi-modemového transceivera[1] v bráne aby správy mohli byť simultánne prijímané na viacerých kanáloch. Hlavné faktory, ktoré ovplyvňujú kapacitu siete sú počet súbežných kanálov, prenosová rýchlosť, payload a ako často uzly vysielajú. Keďže LoRa využíva moduláciu rozšíreného spektra, signály sú prakticky rovnobežné pri použití rozličných faktorov šírenia. Keď sa zmení faktor šírenia, zmení sa aj efektívna prenosová rýchlosť. Brány majú tým pádom výhodu prijímať v rovnakom čase, na rôznych prenosových rýchlostiach, na rovnakom kanály. Ak má uzol dobré spojenie a je blízko k stanici, nieje dôvod aby uzol používal stále najnižšiu prenosovú rýchlosť a obsadzoval tak prístupné spektrum dlhšie ako je potrebné. Tým, že uzol použije vyššiu prenosovú rýchlosť, skráti dobu, ktorú potrebuje na využitie linky a uvoľní tak priestor na komunikáciu pre iné uzly. Adaptívna prenosová rýchlosť tiež optimalizuje životnosť batérie uzlu. Aby adaptívna prenosová rýchlosť mohla fungovať, je potrebné aby bol downlink symetrický s uplinkom a aby mal downlink dostatočnú kapacitu. Tieto vlastnosti zabezpečujú pre LoRaWAN sieť veľkú kapacitu a škálovateľosť. Sieť môže byť spustená s minimálnym množstvom infraštruktúry a keď bude potrebná vyššia kapacita tak sa jednoducho dajú pridať ďalšie brány, čo zabezpečí vyššiu prenosovú rýchlosť a zvýšenie kapacity 6 až 8-krát [2].

3.3.2 Životnosť batérie

Uzly v sieti LoRaWAN sú asynchrónne a komunikujú, keď majú pripavené dáta na odoslanie, či už plánovane, alebo riadené určitou udalosťou. Tento typ protokolu je zvyčajne uvádzaný ako metóda Aloha. V meshovej, alebo synchronizovanej sieti, ako je cellular, musia uzly frekventovane kontrolovať synchronizáciu so sieťou a kontrolovať prijaté správy. Táto synchronizácia konzumuje veľkú časť energie a najviac znižuje životnosť batérie. V porovnaní s inými LPWAN technológiami je práve LoRaWAN 3 až 5-krát účinnejší v šetrení životnosti batérie [2].

[1] Zariadenie, ktoré funguje zároveň ako prijímač aj vysielač.

3.4 Verzie

3.4.1 Verzia 1.0.2

Táto skoršia verzia LoRaWAN protokolu bola špecifikovaná v roku 2016. Aj napriek dostupnosti novšej verzie, mnoho zariadení prácuje stále na verzii 1.0.2. Spätná kompatibilita je najväčšou slabinou tejto verzie, kedy sa pri použití zariadenia s verziou 1.0.2 správa celá sieť podľa staršej verzie.

Na koncovom zariadení sa ukladá niekoľko informácií, ktoré môžu byť rozdelené do dvoch skupín podľa toho či sú na zariadení uložené pred aktiváciou alebo po aktivácii [11].

Informácie na koncovom zariadení pred aktiváciou

- **DevEUI** je globálny identifikátor zariadenia. Je to jedinečné číslo pridelené každému koncovému zariadeniu, podľa ktorého sieťový server rozlišuje jednotlivé koncové zariadenia. Pri aktivácii zariadenia OTAA (Over The Air Activation) je nutné mať túto položku nahratú v pamäti zariadenia, naopak pri ABP (Activation By Personalization) aktivácii to nie je nutné, ale doporučené.
- **AppEUI** je rovnako ako DevEUI globálny identifikátor, ktorý sa používa v rámci Join request operácii a identifikuje sa podľa neho aplikácia, ktorá sa na zariadení používa.
- **AppKey** je aplikačný kľúč s dĺžkou 128 bitov, ktorý sa používa v rámci AES šifrovania. Kľúč je na zariadení uložený v nešifrovanom tvare a používa sa pri aktivácii OTAA na odvodenie relačných kľúčov (AppSKey a NwkSKey). Pomocou týchto kľúčov je následne šifrovaná celá komunikácia zariadenia a sú špecifické pre každé koncové zariadenie.

Informácie na koncovom zariadení po aktivácii

- **DevAddr** je adresa koncového zariadenia dĺžky 32 bitov, ktorá slúži k identifikácii zariadenia v rámci siete. Prideľuje ju sieťový server.
- **NwkSKey** je relačný sieťový kľúč, ktorý je špecifický pre každé koncové zariadenie. Používa ho koncové zariadenie a sieťový server k overovaniu MIC (Message Integrity Code), čo zabezpečuje integritu dát.
- **AppSKey** je relačný aplikačný kľúč, ktorý je rovnako ako NwkSKey špecifický pre každé koncové zariadenie. Používa ho koncové zariadenie a aplikačný server na šifrovanie užitočných dát (payload).

Koncové zariadenia majú dve možnosti aktivácie. Jedná sa o ABP (Activation By Personalization) a OTAA (Over The Air Activation).

Activation By Personalization
Pri tejto forme aktivácie koncového zariadenia sa ručne zadávajú všetky potrebné informácie na server a koncové zariadenie a teda sa nevykonáva pripojovacia procedúra Join-request. Namiesto zadávania informácií, ktoré sa zapisujú do zariadenia pred aktiváciou (DevEUI, AppEUI a AppKey) sa do zariadenia zapisujú priamo údaje po aktivácii (DevAddr, NwkSKey a AppSKey). Potrebné informácie sa okrem koncového zariadenia zadajú aj do sieťového a aplikačného serveru. Jedná sa však o nebezpečnejší spôsob aktivácie po ktorej je sieť náchylnejšia na útok, preto sa nedoporučuje tento spôsob používať mimo izolovanej siete a aj to len v prípade testovania.

Over The Air Activation
V prípade aktivácie koncového zariadenia pomocou OTAA prechádza zariadenie pripojovacou procedúrou vždy po ukončení relácie. Jedná sa o výmenu správ Join-request a Join-accept medzi koncovým zariadením a serverom. Na koncovom zariadení je nutné mať pred samotnou pripojovacou procedúrou uložené informácie DevEUI, AppEUI a AppKey. Pri pripojovacej procedúre si následne sieťový server aj koncové zariadenie dokážu po synchronizácii odvodiť relačné kľúče a sieťový server pošle AppSKey a DevAddr na aplikačný server v zašifrovanej forme.

3.4.2 Verzia 1.1

Novšia verzia protokolu, ktorá bola špecifikovaná v roku 2017. V tejto verzii bola upravená bezpečnosť protokolu, zariadenia triedy B, boli pridané MAC príkazy, zdokonalila sa metóda pripájania a aj roamingová podpora [12].

Upravenie bezpečnosti
V novej verzii protokolu sa nachádza čítač rámcov, ktorý sa počas jednej relácie môže použiť iba raz. Zabraňuje tak útokom počas pripojovania zariadenia a pri posielaní či prijímaní správ. Hodnota tohto čítača rámcov sa ukladá do trvalej pamäte (NVRAM).

Ďalšia zmena sa tíka aktivácie OTAA, kde hodnota AppNonce bola premenovaná na JoinNonce a spolu s hodnotou DevNonce už niesú náhodne generované. Po pripojení sa tieto hodnoty načítavajú a sú uložené v trvalej pamäti. Z tohto dôvodu a dôvodu spomenutého vyššie sa odvodila nutnosť inštalácie napäťovo nezávislej pamäte do zariadení.

Úprava bezpečnosti sa dotkla kľúčov. Okrem kľúča AppKey vznikol aj tajný sieťový kľúč NwkKey, ktorý je obdobou relačného sieťového kľúča a používa sa na generovania troch nových relačných kľúčov (NwkSEncKey, FNwkSIntKey a SNwkSIntKey). NwkSEncKey (Network Session Encryption Key) sa používa na šifrovanie MAC príkazov, FNwkSIntKey (Forwarding Network Session Integrity Key) a SNwkSIntKey (Serving Network Session Integrity Key) sa používajú na výpočet a overenie integrity správ (MIC). Relačný aplikačný kľúč (AppSKey) sa stále odvodzuje z aplikačného kľúča (AppKey), no odvodzovanie všetkých kľúčov je viac komplexnejšie ako pri staršej verzii protokolu.

Zariadenia triedy B

Špecifikácia tejto triedy je jednou s noviniek vo verzii 1.1 protkolu LoRaWAN. Zariadenia triedy A sú zamerané na najvyššiu možnú úsporu elektrickej energie a naopak zariadenia triedy C majú neustále otvorené komunikačné okno čo zvyšuje energetickú spotrebu. Zariadenia triedy B dostávajú synchornizačné pakety čo umožňuje zariadeniu byť v úspornom režime. Brána posiela formou broadcastu beacon synchronizačné rámce na všetky koncové zariadenia. Sieťový server dokáže nakonfigurovať prenosovú rýchlosť a frekvenciu a koncové zariadenie môže informovať sieťový server o výbere najlepšej brány. V prípade pohybu zariadenia je sieť periodicky informovaná o bránach v dosahu a kvalite signálu.

MAC príkazy

Vo verzii protokolu 1.1 pribudlo niekoľko MAC príkazov. MAC príkazy používa sieťový server na konfiguráciu zariadenia a koncové zariadenie pomocou nich môže zistiť informácie zo siete ako ADR (Adaptive Data Rate) či absolútny čas kvôli časovej známke (timestamp). Pribudli nové MAC príkazy pre znovupripojenie k sieťovému serveru, pre zaslanie nových relačných kľúčov a pre roaming.

Pripájanie zariadení

V staršej verzii protokolu LoRaWAN 1.0.2 bolo pred pripojením zariadenia nutné nakonfigurovať informácie DevEUI, AppEUI a AppKey. V novšej verzii protokolu 1.1 sú potrebné informácie JoinEUI, DevEUI, NetworkKey a AppKey. Sieťový server po prijatí požiadavky na pripojenie vyhľadá pripojovací server, ktorý je ďalej zodpovedný za odvodenie relačných kľúčov, ktoré následne pošle na sieťový a aplikačný server.

Roaming

Novinkou vo verzii 1.1 je aj roaming. Protokol LoRaWAN podporuje dva druhy ro-

amingu a to pasívny roaming a handover roaming. Pasívny roaming podporovala aj verzia 1.0 kde sieťový server preposlal pakety na iný sieťový server pre ktorý boli pakety určené a teda celá procedúra nezáležala od koncového zariadenia. Na handover roaming už je potrebná verzia 1.1, pretože koncové zariadenie vie, že sa nejedná o komunikáciu s vlastným domácim sieťovým serverom ale so slúžiacim sieťovým serverom. Profil koncového zariadenia je uložený na domácom serveri a na slúžiacom serveri je zariadenie aktivované. Medzi domácim a slúžiacim sieťovým serverom sa nachádza ešte ďalší, smerovací sieťový server.

Tak ako pri verzi LoRaWAN 1.0.2, tak aj pri verzii 1.1 existujú informácie, ktoré sa ukladajú do zariadenia pred aktiváciou a ďalšie informácie, ktoré sú uložené do zariadenia po aktivácii.

Informácie na koncovom zariadení pred aktiváciou

- **JoinEUI** je globálny aplikačný identifikátor slúžiacia k identifikácii pripojovacieho serveru, ktorý počas pripojovacej procedúry odvodzuje relačné kľúče. Pri aktivácii OTAA je nutné mať túto informáciu uloženú v pamäti zariadenia pred začatím pripojovacej procedúry, naopak pri aktivácii ABP to nutné nie je.
- **DevEUI** je rovnako globálny identifikátor ako JoinEUI. Je to jedinečné číslo, ktoré slúži sieťovému serveru na rozlišovanie jednotlivých koncových zariadení. Táto informácia je potrebná pri oboch spôsoboch aktivácie, kde pri OTAA musí byť táto informácia uložená priamo v pamäti a pri ABP to nie je nutné ale doporučené.
- **Kĺúče AppKey a NwkKey** sú kľúče šifrované pomocou algoritmu AES. Tieto kĺúče sú pre zariadenie špecifikované výrobcom. Pri aktivácii ABP nie sú tieto kľúče potrebné, no pri aktivácii OTAA áno. NwkKey slúži na odvodenie troch relačných kľúčov (NwkSEncKey, FNwkSIntKey a SNwkSIntKey) a ApkKey slúži na odvodenie relačného aplikačného kľúča AppSKey.
- **Kľúče JSIntKey a JSEncKey** sú kľúče, ktoré sa odvodzujú len pri aktivácii OTAA, majú obmedzenú životnosť a sú odvodené z kľúča NwkKey. JSIncKey sa používa na výpočet MIC pri odosielaní správy Rejoin-request a jej odpovedi Join-accept. JSEncKey sa používa na šifrovanie správy Join-accept vygenerovanou na základe správy Rejoin-request.

Informácie na koncovom zariadení po aktivácii

- **DevAddr** je adresa koncového zariadenia zložená z 32 bitov a slúži na identifikáciu zariadenia vrámci siete. Je pridelená koncovému zariadeniu sieťovým serverom.

- **NwkSEncKey** Network Session Encryption Key je relačný sieťový kľúč, ktorý je pre každé koncové zariadenie špecifický. Používa sa na šifrovanie a dešifrovanie MAC príkazov odosielaných ako payload.
- **FNwkSIntKey** Forwarding Network Session Integrity Key je relačný sieťový kľúč, ktorý je pre každé koncové zariadenie špecifický. Používa sa na výpočet MIC alebo jej časti na zaistenie integrity.
- **SNwkSIncKey** Serving Network Session Integrity Key je relačný sieťový kľúč, ktorý je pre každé koncové zariadenie špecifický. Používa sa na overovanie MIC na zaistenie integrity.
- **AppSKey** je relačný aplikačný kľúč, ktorý je pre každé koncové zariadenie špecifický. Používa ho aplikačný server a koncové zariadenie na šifrovanie a dešifrovanie payloadu. Vďaka tomuto kľúču sieťový server nemá možnost meniť a čítať prenášané dáta.

Aktivácia koncového zariadenia

Rovnako ako pri verzii LoRaWAN 1.0.2, tak aj pri verzii 1.1 existujú dva spôsoby aktivácie koncového zariadenia. Jedná sa o ABP (Activation By Personalization) a OTAA (Over The Air Activation). V prípade ABP sa vo verzii 1.1 nenachádzajú žiadne vylepšenia oproti verzii 1.0.2, preto bude popísaná iba vylepšená metóda OTAA.

OTAA je bezpečnejší spôsob aktivácie zariadenia ako ABP. Rovnako ako pri verzii 1.0.2 prechádza zariadenie pripojovacou procedúrou. Rozdiel však nastáva v serveroch, kde je táto procedúra vykonaná. Na rozdiel od verzie 1.0.2, kde bola pripojovacia procedúra vykonávaná na sieťovom serveri, je vo verzii protolu 1.1 vykonávaná na pripojovacom serveri. Na koncovom zariadení je nutné pred začatím pripojovacej procedúry nakonfigurovať informácie ako DevEUI, JoinEUI, NwkKey a AppKey. Aktivačný proces OTAA sa používa na vzájomné overenie koncového zariadenia a siete aby bola zaistená autorizácia správ.

3.5 Sieťová architektúra

Architektúra siete je založená na topológii v tvare hviezdy. Na rozdiel od meshovej architektúry sa šetrí životnosť batérie v koncových zariadeniach, ktoré takto nemusia preposielať dáta iných uzlov na bránu.

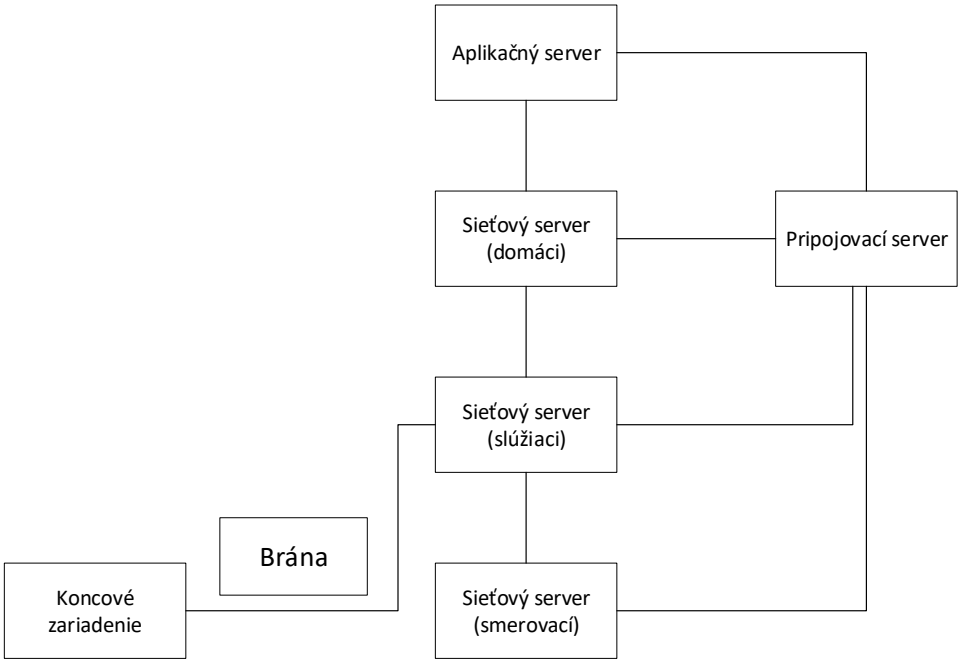
V LoRaWAN sieti nie sú uzly previazané so špecifickou bránou. Naopak, dáta vyslané jedným uzlom sú prijaté niekoľkými bránami. Každá brána potom preposiela prijaté pakety z koncových uzlov na cloudový server cez back-bone[2] sieť (napr.

[2]Back-bone je časť siete, ktorá prepojuje menšie siete dokopy. Funguje ako spojovací uzol medzi

Ethernet, satelit, Wi-Fi či cellular). Server, so svojou inteligenciou a zložitosťou, ovláda sieť, filtruje redundantné prijaté pakety, vykonáva bezpečnostné kontroly, plánuje potvrdenia cez optimálne brány, kontroluje adaptívnu prenosovú rýchlosť, atď. Ak je koncový uzol mobilný, alebo pohyblivý, nie je potrebné aby si brány predávali dáta medzi sebou, čo je kľúčová funkcia na zaistenie sledovania majetku [2].

3.5.1 Referenčný model siete

Na obr. 3.3 môžeme vidieť referenčný model siete LoRaWAN. Sieť sa skladá z koncového zariadenia resp. niekoľkých koncových zariadení, brány, sieťového servera, pripojovacieho servera a aplikačného servera. V prípade domácej LoRaWAN siete býva sieťový server jeden, no v prípade roamingu môže byť sieťových serverov viac (domáci, slúžiaci, smerovací atď.).



Obr. 3.3: Referenčný model siete LoRaWAN [13]

Koncové zariadenie

Koncové zariadenie je tvorené senzorom a je pripojené bezdrôtovo do siete pomocou rádiovej brány. Aplikačná vrstva koncového zariadenia komunikuje so zodpovedným aplikačným serverom v cloude, ktorý spracováva posielané dáta.

menšími LAN sieťami [15].

Rádiová brána

Brána slúži na smerovanie všetkých prijatých paketov z koncových zariadení na sieťový server, ktorý je pripojený cez IP back-bone sieť. Brána funguje iba na fyzickej vrstve a jej úlohou je dekódovať uplinkové rádiové pakety zo vzduchu a posiela ich ďalej v nespracovanej forme na sieťový server. Naopak, pre downlikovú komunikáciu, brána jednoducho pošle pakety zo sieťového servera na koncové zariadenia bez akéhokoľvek zásahu do payloadu.

Sieťový server

Sieťový server predstavuje linkovú vrstvu koncových zariadení v LoRaWAN sieti a je jadrom hviezdicovej topológie. Hlavnými úlohami sieťového servera sú:

- Kontrola adresy koncového zariadenia,
- Kontrola počítadla rámcov a overovanie samotných rámcov,
- Potvrdzovanie,
- Prispôsobovanie prenosovej rýchlosti,
- Vybavovanie všetkých požiadaviek od koncového zariadenia týkajúcich sa linkovej vrstvy,
- Smerovanie uplinkového payloadu na príslušný aplikačný server,
- Zaraďovanie downlinkového payloadu z aplikačných serverov, ktorý sa má ďalej poslať na koncové zariadenia,
- Smerovanie správ Join-request a Join-accept medzi koncovým zariadením a pripojovacím serverom.

V prípade roamingu sa v sieti môže nachádzať sieťových serverov viac, pričom každý z nich plní inú úlohu. Všetko záleží od toho, či je koncové zariadenie v roamingu a aký typ roamingu používa.

Slúžiaci sieťový server riadi linkovú vrstvu koncového zariadenia. V domácom sieťovom serveri sú uložené informácie koncového zariadenia ako profil zariadenia, servisný profil, smerovací profil a DevEUI. Domáci sieťový server je priamo spojený s pripojovacím serverom, ktorý sa používa pri aktivačnej procedúre. Je tiež pripojený na aplikačný server. V prípade, že domáci sieťový server a slúžiaci sieťový server pracujú osobitne, majú medzi sebou roamingovú dohodu. V tomto prípade sú medzi nimi smerované uplinkové a downlikové pakety.

Pripojovací server

Pripojovací server spracováva OTAA aktiváciu koncových zariadení. Na sieťový server môže byť pripojených niekoľko pripojovacích serverov a naopak, pripojovací server môže byť pripojený na niekoľko sieťových serverov.

Koncové zariadenie sa cez Join-request pomocou JoinEUI dotazuje na kon-

krétny pripojovací server. Každý pripojovací server má nastavenú unikátnu hodnotu JoinEUI. Vo verzii LoRaWAN protokolu 1.0.2 sa hodnota JoinEUI nazýva AppEUI. Pripojovací server pozná identifikátor domáceho sieťového servera koncového zariadenia a poskytuje túto informáciu ostatným sieťovým serverom na požiadavku v prípade roamingu.

Pripojovací server má potrebné informácie na spracovanie Join-requestu obdržaného uplinkovou komunikáciou a následne dokáže vygenerovať Join-accept správu a poslať ju downlinkovou komunikáciou. Na tomto serveri tiež prebieha odvodzovanie aplikačných a relačných zabezpečovacích kľúčov. Následne pošle príslušný NwkSKey koncového zariadenia na sieťový server a AppSKey na príslušný aplikačný server. Pripojovací server by mal obsahovať nasledujúce informácie každého koncového zariadenia pod jeho kontrolou:

- DevEUI,
- AppKey,
- NwkKey (iba v prípade koncového zariadenia pracujúcom na verzii LoRaWAN 1.1),
- Identifikátor domáceho sieťového servera,
- Identifikátor aplikačného servera,
- Schopnosť vybrať najlepšiu cestu na komunikáciu s koncovým zariadením,
- Verziu LoRaWAN koncového zariadenia.

Kĺúče NwkKey a AppKey sú prístupné iba na pripojovacom serveri a koncovom zariadení, nikdy sa neposielajú na sieťový či aplikačný server.

Pripojovací server a sieťový server by mali byť schopné sprevádzkovať medzi sebou zabezpečenú komunikáciu, ktorá obsahuje end-point autentifikáciu, ochranu integrity a diskrétnosť. Podobne by mal pripojovací server bezpečne doručiť AppSKey na príslušný aplikačný server. Pripojovací server môže byť pripojený na niekoľko aplikačných serverov a rovnako aplikačný server môže byť prepojený s niekoľkými pripojovacími servermi.

Aplikačný server

Aplikačný server sa stará o celý payload na aplikačnej vrstve priradených koncových zariadení. Generuje tiež celý aplikačný payload pre downlinkovú komunikáciu s koncovým zariadením. Na sieťový server môže byť pripojených niekoľko aplikačných serverov, rovnako tak na aplikačný server môže byť pripojených niekoľko sieťových serverov. Aplikačný server môže byť tiež pripojený na niekoľko pripojovacích serverov. Domáci sieťový server smeruje celú uplinkovú komunikáciu príslušnému aplikačnému serveru na základe DevEUI.

3.6 Bezpečnosť

Je veľmi dôležité aby každá LPWAN technológia disponovala bezpečnosťou. LoRaWAN používa dve bezpečnostné vrsty: jednu pre sieť a druhú pre aplikáciu. Sieťová bezpečnostná vrstva zabezpečuje autenticitu uzla v sieti, zatiaĺ čo aplikačná bezpečnostná vrstva zabezpečuje aby sieťový operátor nemal prístup k aplikačným dátam koncového užívateľa. Používa sa šifrovanie AES s výmenným kľúčom použitím IEEE EUI64 identikikátora [2].

3.6.1 Vlastnosti bezpečnosti

Bezpečnostné riešenie protokolu LoRaWAN je navrhnuté tak aby podporovalo hlavné kritéria protokolu a to nízku spotrebu energie, nízku náročnosť realizácie, nízku cenu a širokú škálovateľnosť. Tým, že zariadenia dané do prevádzky sa používajú dlhú dobu (niekoľko rokov), musí byť bezpečnosť zabezpečená aj do budúcnosti. Bezpečnostný dizajn protokolu dodržiava najmodernejšie princípy: použitý štandard, dobre preverené algoritmy, a end-to-end zabezpečenie.

Počas procesu pripojenia k sieti sa medzi LoRaWAN koncovým zariadením a LoRaWAN sieťou vytvára vzájomná autentifikácia. Vďaka tomu je zabezpečené, že iba overené zariadenia sa môžu pripojiť do siete. Aplikačné a MAC (Media Access Control) správy majú overený pôvod, chránenú integritu, sú chránené pred opakovaním a sú šifrované. Táto ochrana, spojená so vzájomnou autentifikáciou, zaisťuje aby obsah sieťového prenosu nebol zmenený a pochádza od legitímneho zariadenia, tak isto aj to, že nie je možné ho odpočúvať či zachytávať útočníkmi. Bezpečnosť protokolu ďalej zahŕňa aj end-to-end šifrovanie pre aplikačný payload vymieňaný medzi koncovými zariadeniami a aplikačným serverom. LoRaWAN je jeden z mála IoT protokolov, ktorý používa end-to-end šifrovanie. V niektorých tradičných mobilných sieťach je prenos šifrovaný iba keď sa prenáša vzduchom, inak je posielaný ako obyčajný text v chrbtovej sieti operátora. V dôsledku toho sú používatelia zaťažený výberom, používaním a spravovaním ďalšej bezpečnostnej vrstvy (väčšinou vo forme VPN alebo šifrovaním na aplikačnej úrovni). Takéto riešenia sa však vôbec nehodia pre použitie v LPWAN technológii, kde prídavná bezpečnostná zložka značne zvyšuje spotrebu energie, náročnosť a cenu [4].

3.6.2 Implementácia bezpečnosti

Bezpečnostné mechanizmy protokolu LoRaWAN sa opierajú o osvedčené a štandardizované kryptografické algoritmy AES (Advanced Encryption Standard). Tieto algoritmy boli analyzované kryptografickou komunitou po veľa rokov, sú schválené inštitútom NIST [14] (National Institute of Standards and Technology) a sú

široko používané ako najlepšie šifrovacie algoritmy pre uzly a siete. Zabezpečenie LoRaWAN používa AES šifrovanie kombinované s niekoľkými režimami prevádzky: CMAC (Cipher-based Message Authentication Code[3]) pre ochranu integrity a CTR (Counter Mode Encryption[4]) na šifrovanie. Každé LoRaWAN zariadenie je vyrobené s unikátnym 128 bitovým AES kľúčom (AppKey) a globálne unikátnym identifikátorom (EUI-64-based DevEUI). Obe tieto vlastnosti zariadenia sa používajú pri procese overovania zariadenia. Podobne sú aj LoRaWAN siete identifikované podľa 24 bitového, globálne unikátneho identifikátora prideleného od LoRa Alliance [4]. Implementáciu bezpečnosti je možné vidieť aj graficky znázornenú na obr. 3.4.

3.6.3 Zabezpečenie aplikačných dát

Aplikačné dáta sú vždy šifrované end-to-end medzi koncovým zariadením a aplikačným serverom. Ochrana integrity je zabezpečená dvomi krokmi: prvý je ochrana integrity počas prenosu vzduchom poskytnutá LoRaWAN protokolom a druhý je medzi sieťovým a aplikačným serverom použitím zabezpečeného prenosu pomocou protokolov ako sú HTTPS a VPN.

Vzájomné overovanie

Pri aktivácii OTAA sa overuje, že koncové zariadenie aj sieť majú informáciu o AppKey. Overuje sa to na základe výpočtu AES-CMAC[5] (s použitím AppKey) pri požiadavke zariadenia o pripojenie a tiež aj backendovým prijímačom. Ďalej sú odvodené dva kľúče relácie: jeden na zabezpečenie integrity a šifrovania LoRaWAN MAC príkazov a aplikačných dát (NwkSKey) a druhý na šifrovanie end-to-end aplikačných dát (AppSKey). NwkSKey je distribuovaný LoRaWAN sieti pre overenie autentickosti a integrity paketov. AppSKey je potom distribuovaný aplikačnému serveru na šifrovanie a dešifrovanie aplikačných dát. AppKey a AppSKey sú ukryté pre sieťového operátora aby nemohol dešifrovať aplikačné dáta [4].

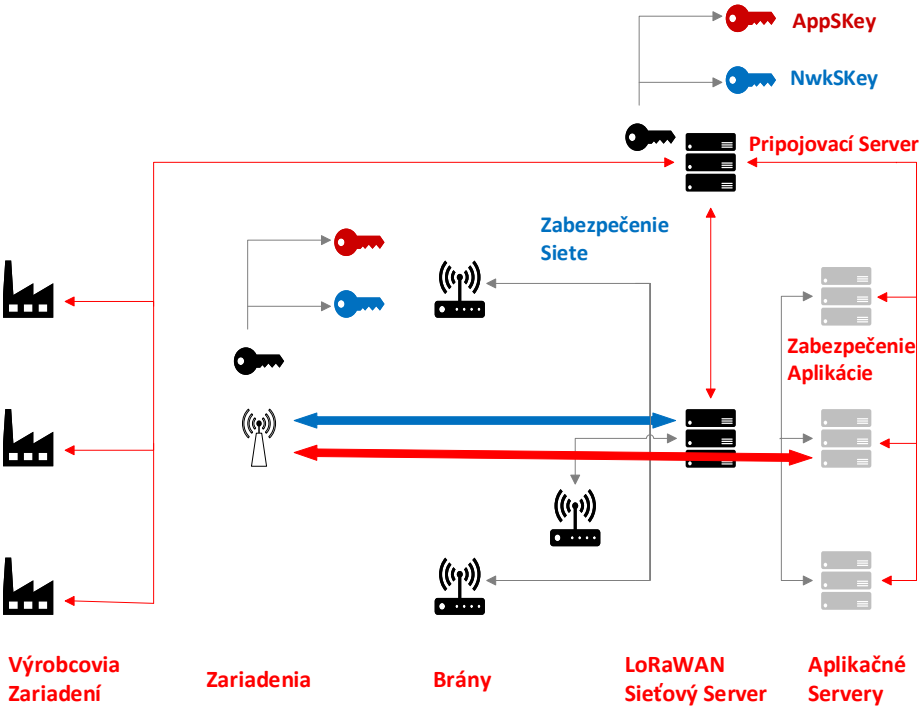
Integrita dát

Všetky LoRaWAN prenosy sú chránené použitím dvoch kľúčov v relácii. Všetky dáta sú šifrované pomocou AES-CTR a obsahujú počítadlo rámcov (používa sa na zamedzenie opakovania paketov) a MIC (Message Integrity Code) vypočítaný pomocou AES-CMAC (aby sa predišlo neoprávnenému zásahu do paketu). Časti LoRaWAN paketu sú zobrazené na obr. 3.5.

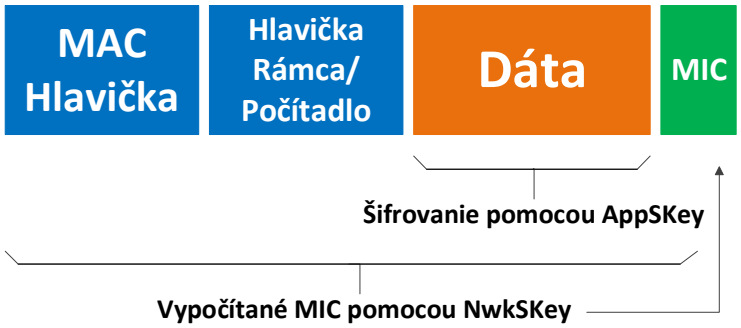
[3]CMAC je šifrovací autentifikačný kód pre správy.

[4]CTR je to režim činnosti algoritmu AES, ktorý sa opiera o počítadlo na šifrovanie toku dát.

[5]CMAC s použitím AES šifrovacieho algoritmu pre zabezpečenie integrity a autentickosti správy.



Obr. 3.4: Zabezpečenie siete LoRaWAN [4].



Obr. 3.5: Štruktúra LoRaWAN paketu a jeho zabezpečenie [4].

4 Bezpečnostné hrozby a scenáre incidentov

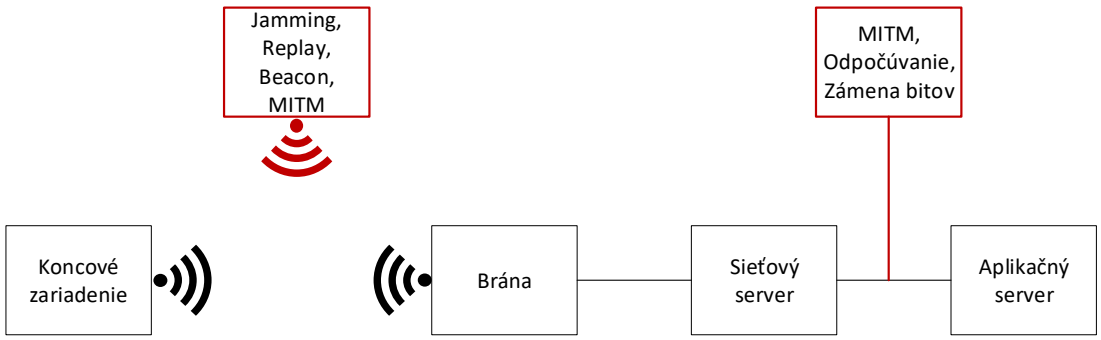
Táto kapitola sa bude venovať najznámejším bezpečnostným hrozbám, ktorým technológia LoRaWAN čelí v praxi. Následne budú popísané scenáre bezpečnostných incidentov niektorých spomenutých hrozieb a možnosti ich detekcie.

4.1 Bezpečnostné hrozby

Účelom tejto práce je detekcia anomálií v LoRaWAN sieťach. Preto budú teraz popísané niektoré najznámejšie bezpečnostné hrozby, ktorým siete LoRaWAN čelia. Tieto hrozby sú vypísané v tab. 4.1 a popísané nižšie. Ich začlenenie v rámci architektúry siete je možné vidieť na obr. 4.1.

Tab. 4.1: Sumár bezpečnostných hrozieb [16]

Bezpečnostná hrozba	**Kategória**	**Sumár**
Rádio-frekvenčné rušenie	DoS	Je obtiažne ochrániť bezdrátové siete pred rušením. Následok je Denial-of-Service (DoS)
Replay útok	MR/DoS	Kombináciou opakovacia správ (MR) a rádio-frekvenčného rušenia dostávame ťažko detekovateľné DoS.
Beacon (Trieda B) synchronizačný útok	DoS	Uzly nedostávajú downlinkové prenosy čo spôsobuje kolízie v prenose.
Analýza sieťového prenosu	TA	Aj bez dešifrovania dát môže analýza prenosu viesť k úniku informácií.
Man-in-the-Middle (MITM) útok	MITM	V prípade nezabezpečenej komunikácie môže dôjsť k odhaleniu tajných kľúcov, keď je napojená komunikácia medzi servermi.



Obr. 4.1: Bezpečnostné hrozby v rámci architektúry siete.

4.1.1 Rušenie rádio-frekvenčného prenosu

Signál môže byť rušený na bráne alebo uzle za pomoci pomerne lacného príslušenstva. Rušenie prenosu vedie k DoS (Denial-of-Service), čo zamedzuje legitímnym

používateľom v korektnom používaní služby. Takýto útok je však ľahko detekovateľný, aj keď niektoré rádio-frekvenčné rušenia sa detekujú pomerne zložito, sú veľmi nebezpečné pre bezdrôtové prenosy a je veľmi obtiažne sa im vyhnúť.

4.1.2 Replay útok

Táto forma útoku je použítá počas pripojovacej procedúry v LoRaWAN sieti a je realizovaná za pomoci techniky selektívneho rádio-frekvenčného rušenia. Útočník môže selektívne rušiť signály (za použitia technológie inteligentného snímania) určené pre OTAA reláciu. Tento útok spôsobí, že prenos žiadosti o pripojenie do siete od legitímneho koncového zariadenia (Join-request č.1 s DevNonce[1] č.1) je rušený a zároveň zachytený útočníkom. Koncové zariadenie čaká po určitú dobu (timeout) na odozvu (Join-accept), ktorú v pri tomto útoku nedostane a potom pošle ďalšiu žiadosť o pripojenie (Join-request č.2) s novou hodnotou DevNonce (DevNonce č.2). Útok včas ruší aj tento prenos. Potom útočník pošle uloženú žiadosť o pripojenie (Join-request č.1). Sieťový server potom overí hodnotu DevNonce (DevNonce č.1) a potvrdí žiadosť. Týmto sa sieťový server, pripojovací server a koncové zariadenia desynchronizujú, čo spôsobí, že odvodené kľúče v relácii sa nebudú zhodovať, keďže sa všetky odvodzujú práve od hodnoty DevNonce.

Tento útok sa používa hlavne od kedy je komunikácia v sieťach LoRaWAN limitovaná. Každé koncové zariadenie má povolený prenos 14 paketov denne (z toho maximálny payload na paket je 12 bajtov) zahŕňajúc potvrdzovanie prijatých uplinkových správ.

Na to aby sa tento útok podaril, musí útočník v rovnakom čase zachytiť paket poslaný z koncového zariadenia a zároveň ho rušiť aby ho pripojovací server nedostal. To je možné dosiahnuť zariadením, ktoré zachytí paket z koncového zariadenia mimo dosahu rušenia rušičkou, čo nieje vždy možné a je to závislé od vzdialenosti k najbližšej bráne. Tento útok je obtiažnejší aj z dôvodu viacerých prijímacích ciest pre koncové zariadenia (jeden paket z koncového zariadenia zachytáva viacero brán), čo je veľmi bežné v sieťach LoRaWAN.

4.1.3 Beacon (Trieda B) synchronizačný útok

Zariadenia triedy B nie sú v tomto smere nijak zabezpečené, čo znamená, že útočník môže prinútiť bránu poslať falošný synchronizačný signál. To spôsobuje, že koncové zariadenia triedy B budú prijímať okná nesynchronizované s bránou čo tiež zvyšuje riziko kolízie vo vysielaných paketoch. Riešenie tohto problému by mohlo byť formou

[1]DevNonce je náhodne vygenerované číslo.

vydania kľúča, ktorý by brány používali na autentifikovanie prenosu synchronizačných signálov.

4.1.4 Analýza sieťového prenosu

Útočník môže nastaviť bránu aby prijímala pakety a odvodzovala z nich informácie. Bez prístupu ku kľúčom nebude útočník schopný dešifrovať obsah paketov, preto použiteľnosť tohto útoku závysi na použitej aplikácii. Napríklad, LoRa sieť v budove na detekciu obsadenosti, môže prepustiť informáciu o úrovni aktivity v budove cez analýzu prenosovej rýchlosti.

4.1.5 MITM

Man-in-the-Middle útok je zameraný na servery, konkrétne sa jedná o útok medzi sieťovým a aplikačným serverom (z toho je odvodený aj názov útoku). Ak sa útočník dokáže dostať ku komunikácii týchto dvoch serverov tak môže odhaliť niektoré nešifrované tajné kľúče. Preto je odporúčané používať šifrovanú komunikáciu medzi servermi, čo však môže zvýšiť chybovosť prenosu.

4.1.6 Ďalšie možné útoky

Odpočúvanie správ
Táto forma útoku je možná pri oboch spôsoboch aktivácie koncového zariadenia (ABP alebo OTAA). Ide o opätovné použitie rovnakej hodnoty z čítača rámcov. Takto môže útočník zachytiť, sledovať a odpočúvať správy, ktoré sú vytvorené jedným relačným kľúčom. Pri tomto útoku dochádza aj k zahadzovaniu správ z koncového zariadenia medzi sieťovým a aplikačným serverom. Aplikačný server tak spracováva staré dáta.

Podobným spôsobom je možné odpočúvať správy v rámci falošnej relácie vytvorenej na sieťovom serveri. V tomto prípade útočník prehráva správu Join-request čím sa vytvorí nová falošná relácia.

Zámena bitov
Tento útok je založený na chýbajúcej ochrane aplikačných dát v rámci end-to-end. Transportná vrstva medzi sieťovým a aplikačným serverom nieje zabezpečená. Útočník tak môže upravovať prenášané dáta.

4.2 Scenáre bezpečnostných incidentov

Táto časť práce je venovaná návrhu dvoch možných scenárov pre testovanie bezpečnostných incidentov v sieťach LoRaWAN.

Na to aby bolo možné tieto hrozby analyzovať je potrebné, myslieť ako útočník, vytýčiť dôvody, kvôli ktorým je na sieť vykonaný útok. Ciele útoku môžu byť rozdelené do dvoch aspektov: ohrozenie vlastností zabezpečenia siete a ohrozenie prostriedkov zabezpečenia siete [5].

Medzi vlastnosti zabezpečenia siete môžeme zaradiť dôvernosť, integritu a dostupnosť. Prostriedky zabezpečenia siete sú najdôležitejšie parametre. V prípade, že sú tieto parametre odhalené, celá sieť môže byť v ohrození. Medzi tieto parametre patria hlavne relačné kľúče NwkSKey a AppSKey, ale aj iné informácie ako napr. AppKey, DevNonce, AppNonce, FrmPayload, DevAddr ai.

V tomto prípade môžeme uvažovať, že útočník získa plnú kontrolu nad sieťou a dokaže zachytiť, porušiť a posielať správy. V sieti LoRaWAN to znamená, že útočník má znalosť o sieti LoRaWAN a jej zariadeniach, dokáže zachytiť a posielať správy vzduchom, spracovávať a uchovávať dáta, šifrovať a dešifrovať správy (pokiaľ odhalil relačné kľúče) a má tiež fyzický prístup k jednotlivým zariadeniam.

4.2.1 Jamming

Tento druh útoku za zaraďuje medzi DoS útoky kedy je cieľom útočníka zamedziť resp. úplne odstaviť použiteľnosť siete LoRaWAN. Počas tohto útoku je útočníkom nastražené zariadenie – jammer, ktoré je možné vytvoriť pomocou obyčajného koncového zariadenia, na ktorom je zvýšený vysielací výkon a neustálym vysielaním zahlcuje prenosovú linku tak aby ostatné zariadenia nedokázali komunikovať s bránou.

Na dosiahnutie útoku s najlepším výsledkom je potrebné poznať umiestnenie brány a jammer umiestniť k bráne čo najbližšie. Tak isto je potrebné poznať frekvenčné pásmo v ktorom sieť pracuje a jammer nastaviť aby pracoval v rovnakom pásme.

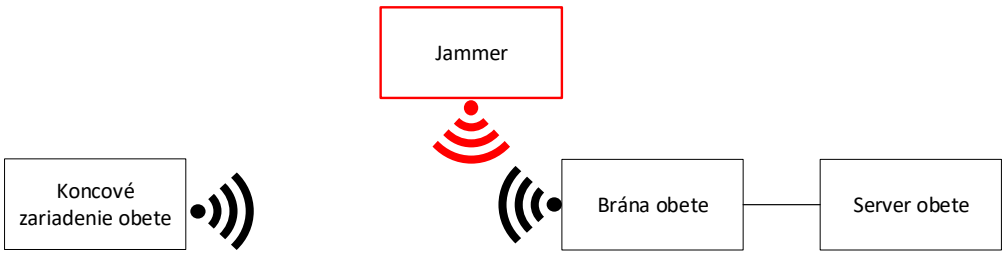
Popis útoku

Na obr. 4.2 je vyobrazený spôsob útoku. Postup môže byť nasledovný:

- Na prvom mieste musí útočník zistiť kde je umiestnená brána siete a na akom frekvenčnom pásme s bránou komunikujú koncové zariadenia.
- V ďalšom kroku je potrebné vybrať vhodné koncové zariadenie, ktoré dokáže vysielať naraz na niekoľkých frekvenciách a faktoroch rozprestrenia. Tiež je vhodné aby sa na zariadení dal zvýšiť vysielací výkon. Výkon, s ktorým jammer vy-

siela a vzdialenosť jammera od brány sú kľúčové aspekty pre efektívne rušenie komunikácie.

- Následne je potrebné do jammera nahrať program, ktorý bude na vysokom výkone neustále vysielať join-request pakety. Pri tomto útoku nieje cieľové poznať kľúče potrebné na komunikáciu v sieti. Cieľom jammingu je týmito správami, ktoré musí brána prijímať, spracovať a preposielať na server zahltiť frekvenčné pásmo a tiež čo najviac zaťažiť server join-request žiadosťami. V tom prípade bude jamming spôsobovať nefunkčnosť jednej brány ale v prípade väčšej siete s viacerými bránami dokáže spôsobiť DoS aj na úrovni servera.
- V poslednom kroku je potrebné už len umiestniť jammer do blízkosti brány.



Obr. 4.2: Jamming

Tento druh útoku je obzvlášť nebezpečný pre menšie siete kde sa používa len jedna brána. V takom prípade je útočník schopný úplne odstaviť sieť. V prípade väčších sietí by útočník musel použiť jammerov viac a to pre každú bránu osobitne aby bol útok maximálne efektívny.

4.2.2 Výpadok pripojenia

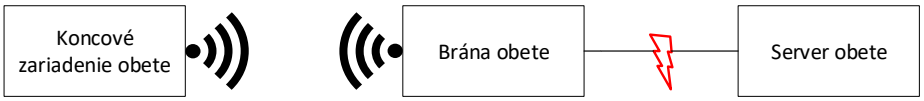
Výpadok pripojenia, konkrétne medzi bránou a serverom, nemusí byť vždy cielený útok. V praxi sa stretávame bežne s výpadkami internetového pripojenia. Najčastejšie je sieť LoRaWAN riešená spôsobom kde je brána spojená so serverom pomocou backbone siete. Aj keď sa pri tomto bezpečnostnom incidente prevažne jedná o bežný výpadok pripojenia, môže byť takýto incident zneužitý aj útočníkmi pre spôsobenie DoS útoku. Ďalej v tejto práci sa bude k tomuto incidentu pristupovať ako by bol spôsobený cielene útočníkom.

Na to aby bol útočník schopný spôsobiť takýto druh útoku je potrebné aby poznal umiestnenie brány. Výpadok sa dá tiež spôsobiť aj na serveri, tie však bývajú väčšinou dobre zabezpečené proti manipulácii nepoverenými osobami, preto je práve brána slabší článok na spôsobenie výpadku.

Popis útoku

Spôsob útoku je zobrazený na obr. 4.3. Postup útoku je pomerne jednoduchý:

- V prvom rade musí útočník zistiť umiestnenie brány, prípadne servera.
- Po zistení umiestnenia musí útočník len pristúpiť k zariadeniu a jednoducho odpojiť, alebo znehodnotiť internetový kábel.



Obr. 4.3: Výpadok pripojenia

Tento druh útoku je podobne ako predchádzajúci nebezpečný hlavne v malých sieťach s jednou bránou. V tomto prípade dochádza k vyradeniu celej siete. Jedná sa o pomerne jednoduchý spôsob DoS útoku. Bohužial pre útočníka, tak ako je jednoduché tento útok vykonať, tak je jednoduché ho aj detekovať a sieť vrátiť späť do normálnej prevádzky.

5 Realizácia praktickej časti

Posledná kapitola práce je venovaná realizácii praktickej časti bakalárskej práce. Na začiatok bude popísané zostrojenie vlastnej siete LoRaWAN s výberom jednotlivých komponentov a ich konfigurácia. Po zostrojení siete budú podľa navrhnutých scenárov bezpečnostných incidentov vykonané útoky na sieť. Na záver budú uvedené navrhnuté riešenia na detekciu vykonaných útokov.

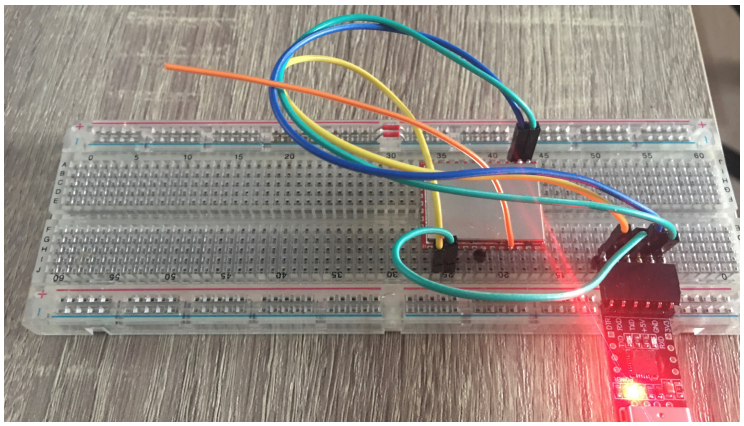
5.1 Zostrojenie siete LoRaWAN

Prvou praktickou časťou práce je zostrojenie samotnej siete LoRaWAN. Táto časť sa bude venovať výberu komponentov siete a ich následnej konfigurácii.

5.1.1 Výber komponentov

V teoretickej časti práce už bolo opísané, že LoRaWAN sieť sa skladá z koncového zariadenia (senzoru), ktoré rádiovo vysiela určité dáta, brány, ktorá dáta poslané zo senzorov prijíma rádiovým prenosom a následne ich po sieti posiela na sieťový server, ktorý ich pošle zodpovednému aplikačnému serveru. Nasledujúca časť práce je venovaná výberu komponentov na zostrojenie LoRaWAN siete.

Koncové zariadenie
Ako koncové zariadenie bol zvolený modul RHF76-052 [18] z dôvodu kvalitnej dokumentácie, veľkej sady príkazov a možnosti rozsiahlejšej možnosti konfigurácie oproti oficiálnemu chipu RN2483 [19]. Modul pracuje na frekvencii 868 MHz, je osadený na nepájivom poli a konfigurácia prebieha pomocou sériového programátora CP2102 [20]. Koncové zariadenie je zobrazené na obr. 5.1.



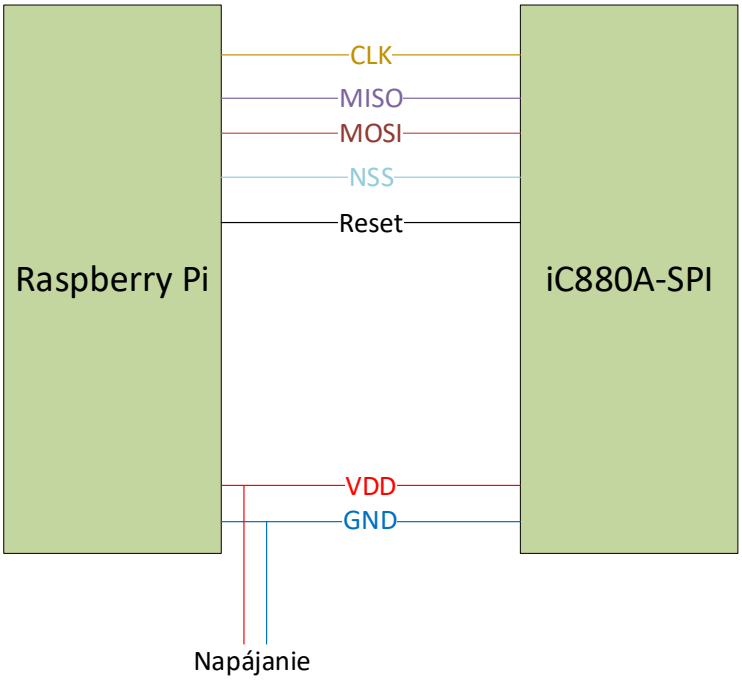
Obr. 5.1: Modul RHF76-052.

Brána

Hardware brány sa skladá z niekoľkých súčastí, ktoré boli vybrané na základe najlepšej dostupnosti samotného hardwaru a dokumentácií.

Základnú dosku brány tvorí single-board počítač Raspberry Pi 3 Model B+ [21]. Väčšina brán používaná v praxi je postavená práve na tomto zariadení, má výbornú technickú podporu, najlepšiu dostupnosť na trhu a širokú možnosť použitia.

K Raspberry Pi je pomocou SPI[1] rozhrania pripojený koncentrátor iC880A [22] podľa obr. 5.2. Pracuje na frekvencii 868 MHz a dokáže prijímať pakety na rôznych faktoroch rozprestrenia až na ôsmich kanáloch súčasne. Ku koncentrátoru je tiež pripojená anténa pracujúca na frekvencii 868 MHz pomocou pigtail kábla.



Obr. 5.2: Prepojenie RaspberryPi a koncentrátora iC880A [24].

Server

Sieťový a aplikačný server boli spolu s bránou nakonfigurované na zariadení Raspberry Pi. Nejedná sa teda o samostatný hardwarový prvok, preto bude konfigurácia servera popísaná v ďalej v texte.

5.1.2 Zostrojenie siete

V tejto časti je popísané zostrojenie kompletnej siete LoRaWAN pomocou komponentov popísaných v predošlej časti práce. Pri zostrojovaní siete LoRaWAN bola po-

[1]SPI (Serial Periphetal Interface) je rozhranie pre synchrónnu sériovú komunikáciu na krátku vzdialenosť primárne používané pre vstavané systémy[23].

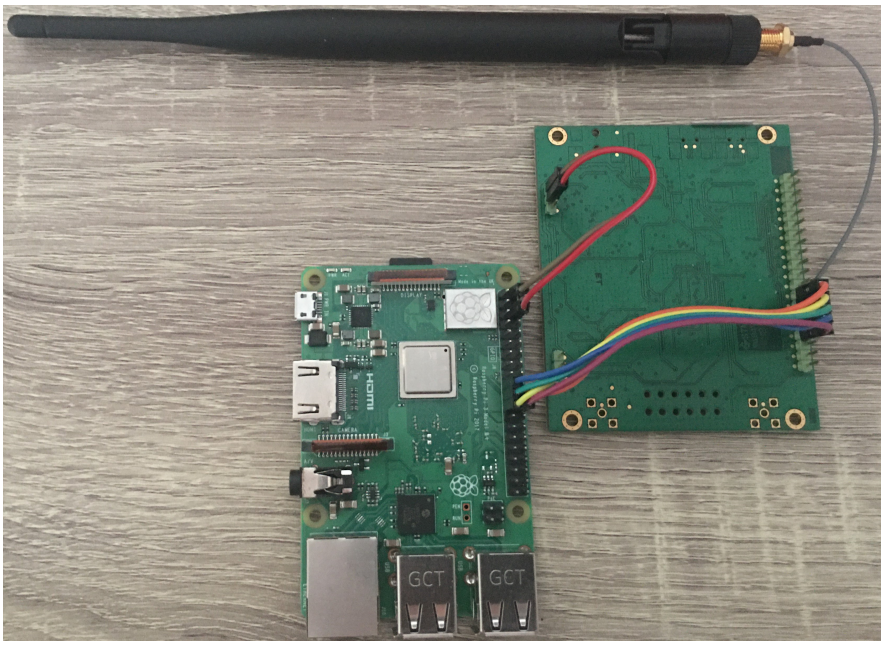
užitá verzia protokolu 1.0.2. Staršia verzia je použitá hlavne z dôvodu bezpečnostných medzier v správe relácií, v pripojovacej procedúre, v mechanizmoch potvrdzovania správ a v rámci integrity. V novšej verzii protokolu 1.1 je už väčšina týchto medzier v bezpečnosti vyriešená. Práca sa venuje detekcii anomálií, preto bude jednoduchšie tieto anomálie pozorovať na staršej verzii protokolu LoRaWAN.

V rámci spätnej kompatibility sa celá sieť správa ako verzia 1.0.2. Pre pripojenie koncového zariadenia je použitá procedúra OTAA, kedy sú na serveri nakonfigurované určité parametre ako aj na koncovom zariadení a relačné kľúče sa následne odvodzujú. Kontrolu a výpočet MIC spolu so šifrovaním vykonáva sieť ako verzia 1.0.2 a ochrana proti prehrávaniu správ nie je použitá.

Konfigurácia servera a brány

Sieťový aj aplikačný server spolu s bránou fungujú spoločne na zariadení Raspberry Pi ako bolo spomenuté už v predošlej kapitole. Na Raspberry bol nainštalovaný operačný systém Raspbian, ktorý funguje na Linuxovom jadre. Ako prvá bola nakonfigurovaná brána. Na to aby Raspberry správne komunikovalo s koncentrátorom bolo potrebné nainštalovať ovládač koncentrátora a pomocou skriptu zabezpečiť aby bol pri každom zapnutí zariadenia vyslaný impulz na resetovací pin koncentrátora.

Pre konfiguráciu serverov bolo použité open-source riešenie Chirpstack [25]. Pre správnu funkciu servera bolo na začiatok potrebné nainštalovať mqtt broker. Následne boli stiahnuté konfiguračné súbory pre komunikáciu brána-server (Gateway-Bridge) a pre sieťový aj aplikačný server. Nakoniec bolo potrebné nakonfigurovať komunikáciu medzi bránou a serverom. To bolo zabezpečené nainštalovaním nástroja packet-forwarder. V skripte tohto nástroja bolo potrebné len nastaviť IP adresy zvolené pre komunikáciu medzi bránou a serverom. V tomto prípade, kedy je brána aj server na jednom zariadení bola zvolená localhost adresa zariadenia a skript pre spúšťanie packet-forwardera bol spojený s vyššie spomenutým skriptom pre resetovací pin koncentrátora tak aby sa automaticky spustil po zapnutí zariadenia. Pre pohodlnejšiu konfiguráciu a následnú správu zariadenia bol použitý program VNC viewer, ktorý funguje ako pripojenie na vzdialenú plochu. Vďaka tomuto programu bolo možné nastaviť a používať Raspberry bez nutného pripájania vstupno-výstupných zariadení. Raspberry Pi disponuje aj WiFi adaptérom vďaka čomu je nutné zabezpečiť iba napájanie a zariadenie sa môže naplno používať. Zariadenie je zobrazené na obr. 5.3.



Obr. 5.3: Raspberry Pi s koncentrátorom iC880A

Konfigurácia koncového zariadenia
Ako bolo spomenuté už v predošlej časti, modul RHF76-052 je pripojený cez sériový programátor k počítaču. Zariadenie sa konfiguruje pomocou AT príkazov, v tomto prípade pomocou nástroja Hercules [27]. Na zariadení bolo potrebné definovať frekvenciu, faktor rozprestrenia a spôsob aktivácie OTAA. Následne bolo potrebné nastaviť pre zariadenie v rámci OTAA aktivácie DevEUI, DevAddr a AppKey. Tieto údaje bolo rovnako potrebné zadať na server. Po vyslaní join-requestu server odvodil relačné kľúče, ktorými sa ďalej šifrovala celá komunikácia a koncovému zariadeniu poslal naspäť join-accept paket. Tým bola aktivačná procedúra úspešne ukončená a koncové zariadenie mohlo posielať šifrované správy na server a opačne.

5.2 Útoky na sieť

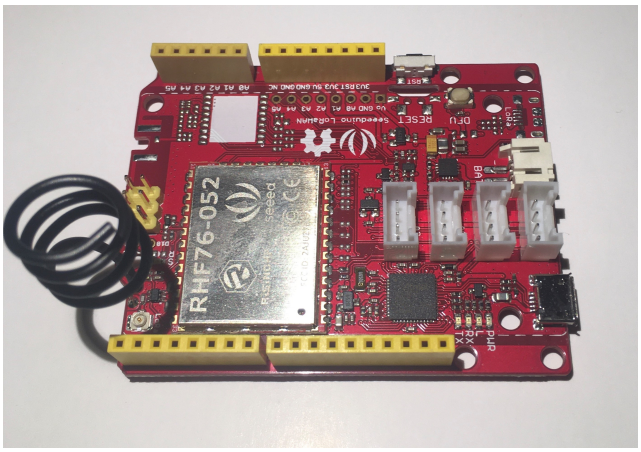
Táto časť popisuje útoky na spravenú sieť LoRaWAN. Na vykonanie útokov boli použité navrhnuté scenáre popísané v predchádzajúcej kapitole. Jeden z útokov je rozsiahlejší – jamming, a jeden menší – výpadok pripojenia.

5.2.1 Jamming

Za účelom návrhu detekcie útokov bol na sieť LoRaWAN vykonaný jamming útok. Jamming, ako bolo už spomenuté pri návrhu scenárov bezpečnostných incidentov,

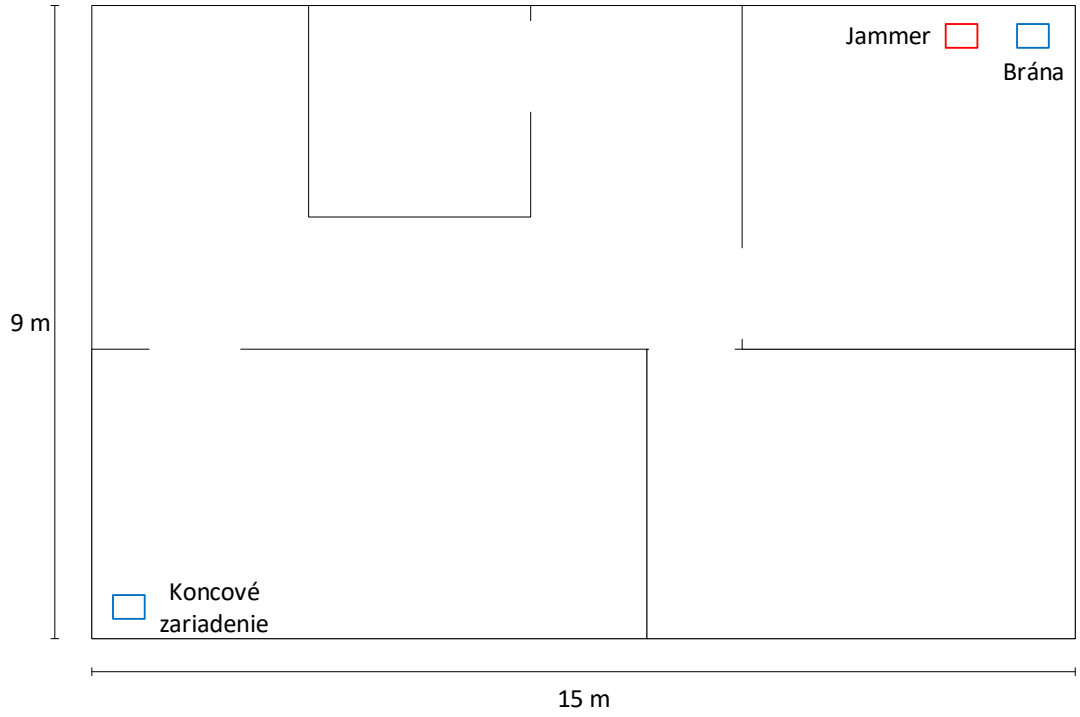
spôsobuje v sieti DoS. Táto forma útoku je obzvlášť nebezpečná pri malých LoRaWAN sieťach kde sa používa len jedna brána. Vytvorená sieť v rámci tejto práce disponuje tiež len jednou bránou. V rámci práce bolo cieľové pomocou jammeru zarušiť komunikáciu koncového zariadenia počas pripojovacej procedúry. Vykonanie pripojovacej procedúry koncového zariadenia je nutné pred každým započatím komunikácie koncového zariadenia so serverom. Zarušenie tejto procedúry teda spôsobí, že koncové zariadenie obete nebude schopné komunikovať so serverom a teda dojde k DoS v sieti.

Na to aby sa mohol zahájiť jamming bolo v prvom rade potrebné vybrať vhodné zariadenie pre jammer. Pre tento účel bolo vybrané zariadenie Seeeduino, ktoré disponuje rovnakým modulom ako koncové zariadenie obete – RHF76-052. Jedná sa o obyčajné konové zariadenie, má dobrú dostupnosť na trhu a jednoduchú konfiguráciu pomocou vývojového prostredia Arduino IDE [28]. Zariadenie je zobrazené na obr. 5.4.



Obr. 5.4: Jammer – Seeeduino

Pred samotným vykonaním útoku bol na koncovom zariadení obete znížený vysielací výkon za účelom nasimulovania používania siete v praxi. Siete LoRaWAN slúžia pre komunikáciu zariadení na vysokú vzrialenosť, preto sa predpokladá, že v praxi je vzdialenosť koncového zariadenia od brány niekoľko desiatok, až stoviek metrov, prípadne jednotiek kilometrov. Pri vykonávaní tohto útoku bolo koncové zariadenie so zníženým vysielacím výkonom umiestnené do inej miestnosti ako bola umiestnená brána. Rozloženie zariadení je zobrazené na obr. 5.5. Týmto spôsobom boli nasimulované aj prekážky (budovy, stromy, múry), ktorým komunikácia siete LoRaWAN čelí v praxi.



Obr. 5.5: Umiestnenie zariadení

Postup útoku bol nasledovný:

- Zariadenie Seeeduino komunikovalo s počítačom pomocou USB zbernice. Konfigurácia bola vykonaná vo vývojovom prostredí Arduino IDE[2].
- V rámci konfigurácie bol na zariadení nastavený najväčší možný vysielací výkon. Okrem toho je potrebné nastaviť hodnotu AppKey. Predpokladá sa, že útočník nepozná túto hodnotu, preto bola táto hodnota náhodne vygenerovaná. Ďalej boli nastavené kanály na ktorých zariadenie pracuje. Tie sa zhodovali s kanálmi na ktorých pracovalo zariadenie obete. Nakoniec bolo nastavené, aby jammer posielal v nekonečnej slučke pakety join-request.
- Po správnom nakonfigurovaní, bol jammer umiestnený do bezprostrednej blízkosti k bráne.
- Jammer sa spustil po prijení k napájaniu pomocou USB kábla. Zariadenie Seeeduino je v praxi možné použiť aj s vlastnou batériou, ktorá sa dá pripojiť k základnej doske.
- Po spustení jammeru boli na server poslané testovacie pakety typu join-request z koncového zariadenia. Tieto pakety neboli zachytené bránou a teda sa nedostali ani na server. Jammer teda fungoval správne, útok bol úspešný a v sieti došlo k DoS.

[2]Zdrojový kód pre jammer sa nachádza medzi prílohami k práci.

5.2.2 Výpadok pripojenia

Ako druhý, menej rozsiahli útok, bol v sieti nasimulovaný výpadok pripojenia brány k serveru. Ako bolo už v práci spomenuté, táto forma incidentu môže byť cielená útočníkom, ale môže sa jednať aj o bežný výpadok v backbone sieti.

Fyzická realizácia tohto incidentu bola vykonaná ešte v rámci semestrálnej práce. Vlastná sieť LoRaWAN bola však v rámci semestrálnej práce nakonfigurovaná mierne odlišne. Rozsiel bol v tom, že LoRa server nebol nakonfigurovaný pomocou open-source riešenia Chirpstack, ale pomocou hotového riešenia od poskytovateľa Loriot. Rozdiel teda spočítaval v komunikácii medzi bránou a serverom, ktorá v rámci semestrálnej práci prebiehala po backbone sieti. V prerobenej sieti, teda v súčastnej konfigurácii, kedy je server spustený spolu s bránou na jednom zariadení, funguje komunikácia pomocou sieťového rozhrania localhost[3]. V tejto konfigurácii je takmer nemožné aby zlyhala komunikácia medzi bránou a serverom, preto sa v rámci tohto útoku bude k sieti pristupovať ako by bola v predošlej konfigurácii.

Brána bola k backbone sieti pripojená pomocou Ethernetového kábla. Celá komunikácia fungovala tak, že brána prijala paket od koncového zariadenia pomocou bezdrôtovej komunikácie a poslala ho ďalej na Loriot server po backbone sieti.

Postup útoku bol v tomto prípade veľmi jednoduchý. Pre realizáciu nieje potrebné žiadne ďalšie zariadenie ani nástroj, resp. v prípade, že nieje priamo dostupný konektor budú potrebné štikacie kliešte. Jediné čo potencionálny útočník potrebuje k realizácii útoku je fyzický prístup k zariadeniu brány. Na výpadok pripojenia je potrebné len vytiahnuť kábel z konektoru brány, prípadne kábel prestrihnúť kliešťami. Po tomto úkone nebude brána schopná komunikovať so serverom a dôjde k DoS.

5.3 Návrh detekcie bezpečnostných incidentov

Poslednou súčasťou práce je návrh detekcie zrealizovaných bezpečnostných incidentov. Predložené návrhy sú prispôsobené tak, aby vlastník siete, resp. administrátor dokázal zistiť, že sieť je napadnutá útočníkom. Po zistení anomálií je nutné aby administrátor našiel zdroj útoku a vykonal potrebné opatrenia na jeho odstránenie.

5.3.1 Detekcia jamming útoku

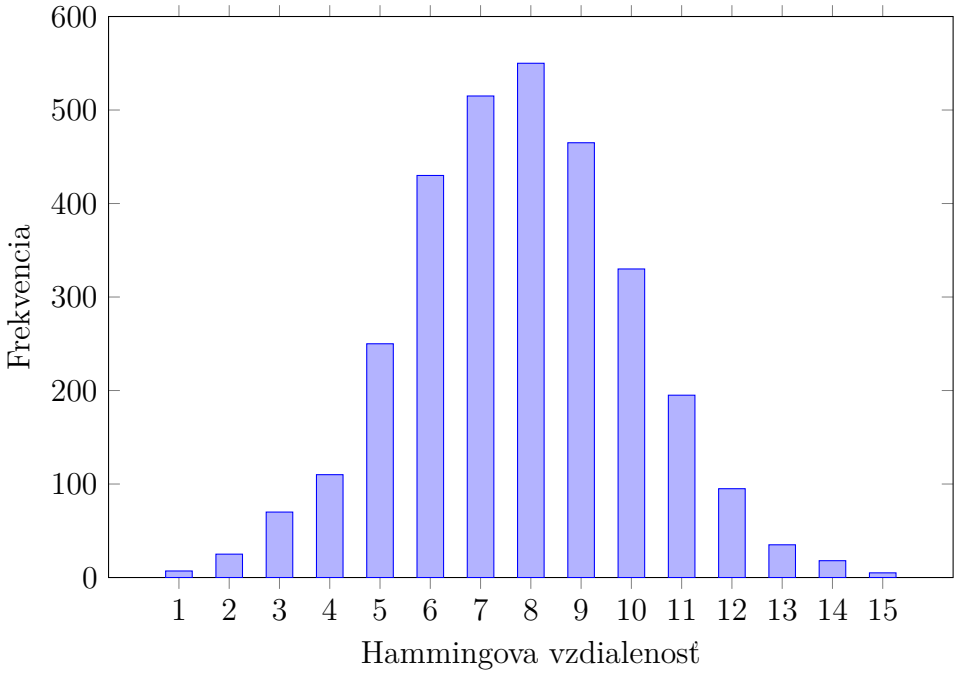
Po zostrojení siete LoRaWAN bol vykonaný jamming útok, ktorý zarušil pripojovaciu procedúru koncového zariadenia. Nefungovala teda end-to-end komunikácia medzi koncovým zariadením a serverom, čo spôsobilo DoS.

[3]Jedná sa o virtuálne sieťové rozhranie v zariadení. Využívajú ho sieťové aplikácie, ktoré pomocou tohto virtuálneho portu komunikujú medzi sebou na rovnakom zariadení.

Na to aby mohol byť navrhnutý spôsob detekcie rušenia pripojovacej procedúry bolo potrebné bližšie pochopiť ako funguje pripojovacia procedúra. Pri aktivácii pomocou OTAA procedúry musí mať koncové zariadenie nastavené DevEUI a AppKey. Tieto hodnoty musia korešpondovať s hodnotami, ktoré sú zapísané na serveri. Koncové zariadenie vyšle join-request, ktorý okrem týchto dvoch premenných obsahuje aj identifikátor join-request paketu a hodnotu DevNonce. DevNonce je 16-bitové, náhodne generované číslo koncovým zariadením, ktoré sa generuje pri každej pripojovacej procedúre. Práve hodnota DevNonce bude ďalej kľúčová pre detekciu jamming útoku.

Hodnota DevNonce sa generuje pomocou n-početnej operácie čítania LSB (Least Significant Bit) registru RegRssiWideband (adresa registra je 0x2c). Hodnota tohto registra je získaná zo sily širokopásmového signálu (4MHz) na prijímači každú 1 ms. Predpokladá sa, že hodnota LSB sa konštantne a náhodne mení v závislosti na kvalite signálu [29].

Graf 5.1: Hammingova vzdialenosť dvoch po sebe prijatých join-request paketov.



Detekcia je založená na výpočte Hammingovej vzdialenosti[4] medzi DevNonce novo prijatého join-request paketu a DevNonce posledne prijatého join-request paketu. Týmto algoritmom sa dajú zistiť základné hodnoty hammingovej vzdialenosti po sebe idúcich hodnôt DevNonce. Tieto hodnoty sú ďalej použité ako hraničné na detekciu jammeru v sieti. Naviac, join-request pakety sú podpísané kľúčom AppKey na zabezpečenie integrity. Útočník by potreboval poznať hodnotu AppKey aby

[4]Hammingova vzdialenosť medzi dvoma číslami je počet pozícii, v ktorých sa dva čísla v binárnej podobe odlišujú [30].

dokázal vypočítať hodnotu MIC join-request paketu aby vedel zistiť základné hodnoty Hammingovej vzdialenosti, čo je pre útočníka príliš zložité. Na to aby útočník spôsobil DoS útok potrebuje hodnotu DevNonce stále rovnakú. Aj v prípade, že útočník pozná základné hodnoty Hammingovej vzdialenosti, tak hraničné hodnoty stále nebude poznať a jammer bude detekovaný kvôli malej hodnote Hammingovej vzdialenosti medzi aktuálnou a predošlou hodnotou DevNonce. V grafe 5.1 sú zobrazené základné hodnoty Hammingovej vzdialenosti zostrojenej siete.

Na detekciu jammingu v sieti bol navrhnutý program (parser[5]), ktorý bol umiestnený na bránu LoRaWAN. Program bol napísaný v jazyku Python.
Postup práce parseru je nasledovný:

- Vstupné hodnoty parseru boli brané z logov programu packet-forwarder priamo z terminálu. Výpis logu programu packet-forwarder:

```
INFO: Received pkt from mote: A50101A5 (fcnt=28324)
JSON up: {"rxpk":[{"tmst":14980140,"chan":4,"rfch":
0,"freq":867.3,"stat":1,"modu":"LORA","datar":"SF12
BW125","codr":"4/5","lsnr":-17.5,"rssi":-108,"size"
:20,"data":"QKUBAaXApG4FhwzQ/w0ADxiAVz4="}]}
INFO: [up] PUSH_ACK received in 10 ms
JSON up: {"stat":{"time":"2020-03-26␣16:36:48␣GMT",
"rxnb":1,"rxok":1,"rxfw":1,"ackr":100.0,"dwnd":0,"t
xnb":0}}
```

- Po načítaní logu je text prehľadávaný a je vybratý záznam, ktorý obsahuje príznak, že paket bol bránou poslaný na server ("JSON up:") a príznak, že sa jednalo o dátový paket ("rxpk"). Z tohto paketu je následne na ďalšie spracovanie vybraný už len payload ("data"). O tieto úkony sa starajú funkcie:

```
def parse_line(line):
    line = line.strip()
    match = re.search(r'JSON␣up:\s*(?P<json_data>.*)',
    line)
    if match:
        request_data = json.loads(match.groupdict()
        ['json_data'])
        return get_rf_payload_from_request
        (request_data)
def get_rf_payload_from_request(request_data):
    if 'rxpk' in request_data.keys():
        return request_data['rxpk'][0]['data']
```

[5]Zdrojový kód pre parser sa nachádza medzi prílohami k práci.

- Payload je preložený do hexadecimálneho formátu:

```
def get_join_request_nonce(rf_payload):
    rf_bytes = bytes(rf_payload.encode('utf-8'))
    rf_decoded_bytes = base64.b64decode(rf_bytes)
    rf_hex = ''.join('{:02x}'.format(ord(x))
    for x in reversed(rf_decoded_bytes))
```

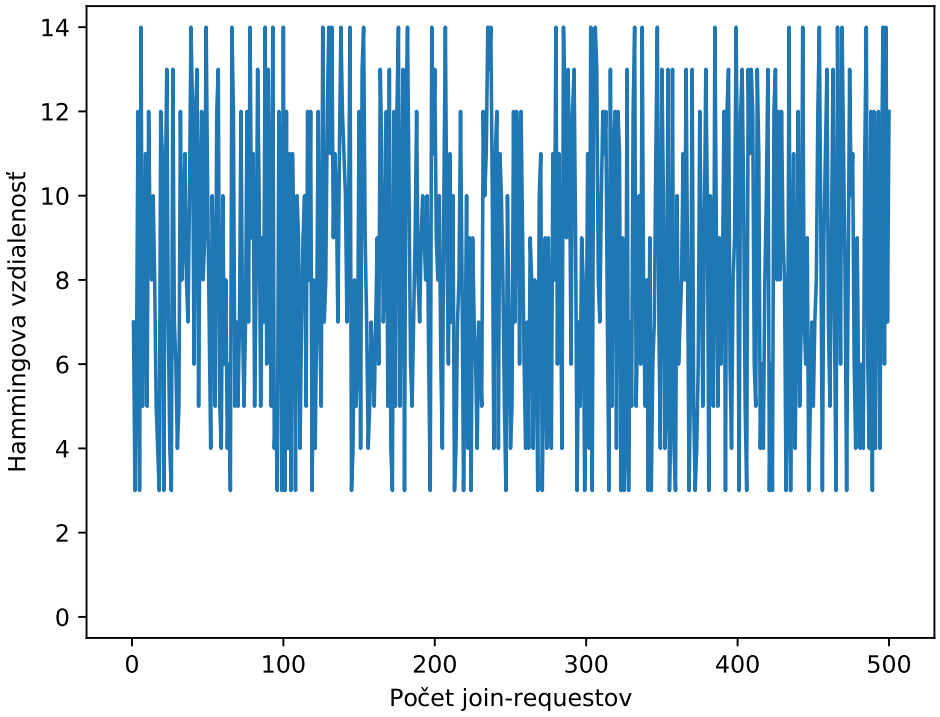
- Nasleduje kontrola, či sa jedná o join-request paket. Join-request paket je špecifický tým, že má dĺžku presne 46 hexadecimálnych znakov. Okrem je join-request označení identifikátorom. Sú to posledné dva hexadecimálne znaky s hodnotou "00". Pokiaľ mal analyzovaný paket inú dĺžku, alebo nebol identifikovaný ako join-request tak ho parser ďalej neanalyzoval. Ak sa jednalo o join-request tak bola z payloadu vybraná hodnota DevNonce na ďalšie spracovanie:

```
    if len(rf_hex) != 46:
        return
    garbage = rf_hex[0:7]
    nonce_hex = rf_hex[8:12]
    dev_eui = rf_hex[12:28]
    app_eui = rf_hex[28:44]
    request_type = rf_hex[44:]
    if request_type != '00':
        return
    nonce = int(nonce_hex, 16)
    return nonce
```

- Nakoniec sa z novo získanej, a predošle získanej hodnoty DevNonce vypočíta Hammingova vzdialenosť a zaznačí sa do grafu závislosti Hammingovej vzdialenosti na počte paketov. Graf sa obnovuje po každých 50 paketov a po dosiahnutí 500 paketov sa cyklicky nahradzuje:

```
def plot_hammings(hammings):
    plt.plot([i for i in range(len(hammings))],
    hammings)
    plt.xlabel('Počet␣join-requestov')
    plt.ylabel('Hammingova␣vzdialenosť')
    plt.savefig('plots/hammings.pdf')
    out_name = 'plots/' +
    str(int(round(time.time() * 1000))) + '.pdf'
nonces = []
hammings = []
```

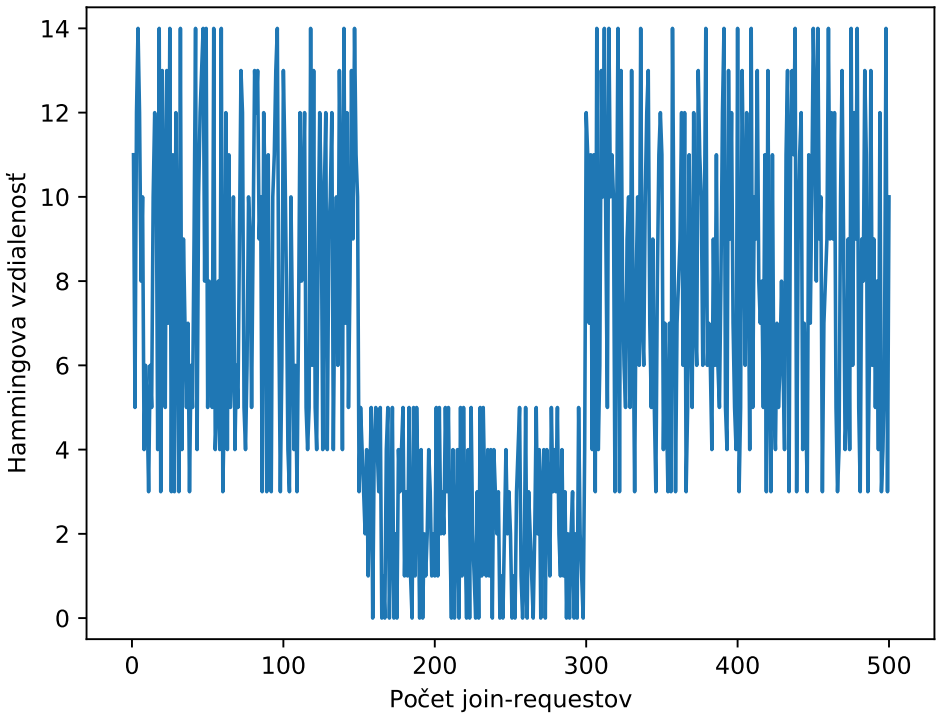
```
for line in sys.stdin:
    rf_payload = parse_line(line)
    if rf_payload is None:
        continue
    nonce = get_join_request_nonce(rf_payload)
    if nonce is None:
        continue
    nonces.append(nonce)
    if len(nonces) > 1:
        last_two = nonces[-2:]
        hamming_distance = bin(last_two[0]
        ^ last_two[1]).count('1')
        hammings.append(hamming_distance)
        if len(hammings) % 50 == 0:
            print('asdf')
            plot_hammings(hammings)
        if len(hammings) == 500:
            hammings = hammings[50:]
```



Obr. 5.6: Hammingová vzdialenosť pri normálnej prevádzke.

Na obr. 5.6 je zobrazený výstup detekčného programu pri normálne fungujúcej sieti. Z grafu je zrejmé, že hodnoty Hammingovej vzdialenosti sa pohybujú v rozmedzí základných hodnôt (3–14).

Vďaka nízkej hodnote Hammingovej vzdialenosti je možné v sieti detekovať jammer. Na obr. 5.7 je zobrazený výstup detekčného programu za prítomnosti jammeru. Z grafu je zrejmé, že k jammingu dochádzalo v čase medzi 150. až 300. join-request paketom.



Obr. 5.7: Hammingova vzdialenosť za prítomnosti jammeru.

5.3.2 Detekcia výpadku pripojenia

Ako bolo už niekoľko krát spomenuté, k výpadku pripojenia nemusí dojsť len v prípade cieleného útoku. Výpadok môže nastať aj v bežnej prevádzke, napr. v dôsledku údržby v backbone sieti. Preto je vhodné aby bola sieť na určitej úrovni monitorovaná stále pomocou rôznych sieťových nástrojov. Na monitorovanie sieťovej komunikácie môže slúžiť napr. veľmi rozšírený program Wireshark [31]. Pomocou tohto programu sa dá jednoducho detekovať výpadok pripojenia brány.

Postup detekcie je nasledovný:

- Na bránu bol nainštalovaný sieťový nástroj Wireshark a následne bol hneď spustený, čím sa započalo zachytávanie paketov.
- Nasimuloval sa výpadok pripojenia odpojením Ethernetového kábla z brány, čím sa prerušila komunikácia so serverom.
- Hneď po výpadku program detekoval neúspešne zaslané pakety, ktoré sa brána snažila odoslať.

V prílohe A.1 je zobrazená zachytávaná prevádzka na bráne. Z obrázku možno vyčítať, že brána komunikovala bez problémov do približne 50. sekundy, kedy brána odoslala TLS paket (paket 31) na Loriot server. Paket je zobrazený v prílohe A.2. TLS protokol pracuje s TCP segmentom a teda sa jedná o zabezpečený druh komunikácie, kedy je očakávaný od príjemcu potvrdzovací ACK paket. Paket sa však nepodarilo doručiť, preto bol niekoľko krát ešte preposlaný (pakety 32–35). Preposielanie však tiež nebolo úspešné. Následne, bol ešte úspešne zaslaný TCP paket (paket 36). Po úspešnom odoslaní tohto paketu došlo k výpadku. Výpadok je možné detekovať podľa ARP paketov (pakety 38–40), kedy sa LoRaWAN brána dotazuje na sieťovú bránu lokálnej siete (router). Nakoniec je zobrazený ešte jeden neúspešný pokus o preposlanie TLS paketu. Výpadok pripojenia v tomto prípade môže administrátor detekovať pomocou ARP paketov, kedy je zjavné, že LoRaWAN brána nedokáže komunikovať so sieťovou bránou v lokálnej sieti.

Záver

Bakalárska práca bola venovaná LPWAN technológii LoRaWAN. Na začiatku práce je vo všeobecnosti popísaný koncept internetu vecí, jeho technológia, štruktúra a používané komunikačné protokoly. Ďalej bola popísaná technológia LPWAN so zameraním na štruktúru a požiadavky tejto technológie. Technológia je zameraná na bezdrôtovú komunikáciu zariadení na veľkú vzdialenosť s nízkou spotrebou energie. V rámci toho boli opísané tri najpoužívanejšie protokoly v praxi: Sigfox, NB-IoT a LoRaWAN.

V práci je venovaná kapitola detailnému opisu technológie LoRaWAN, rozboru fyzickej vrstvy LoRa modulácie a linkovej vrstvy protokolu. V rámci linkovej vrstvy LoRaWAN je možné zariadenia rozdeliť do troch skupín (A, B a C) podľa využitia. LoRaWAN musí spĺňať určité parametre v rámci LPWAN technológie ako je veľký dosah a nízka spotreba energie. Ďalej sú popísané verzie protokolu, kde sú porovnané dve verzie 1.0.2 a 1.1. Verzia 1.1 má oproti staršej verzii 1.0.2 mnoho vylepšení zameraných hlavne na bezpečnosť siete. Je tu popísaná sieťová architektúra kde sú bližšie opísané jednotlivé zariadenia používané v sieti LoRaWAN. Vo všeobecnosti sa jedná o koncové zariadenia, brány a rôzne typy serverov: aplikačný, sieťový a pripojovací. Z teoretického hľadiska je v poslednom rade opísaná bezpečnosť siete kde je spomenutá aktivačná procedúra koncových zariadení a šifrovacie kľúče použité na zabezpečenie prenášaných dát. Kapitola obsahuje najznámejšie útoky na sieť LoRaWAN kde sú popísané spôsoby útokov a ich následky.

Teoretická časť práce je ukočená analýzou najznámejších útokov, ktorým siete LoRaWAN čelia v praxi a návrhom scenárov pre testovanie bezpečnostných incidentov. Jedná sa o útoky typu DoS – jamming a výpadok pripojenia v backbone sieti.

V rámci praktickej časti tejto práce bola najprv zostrojená sieť LoRaWAN. V tejto kapitole práce je popísaný výber komponentov použitých na zostrojenie siete a ich následná konfigurácia. Ako koncové zariadenie bol použitý modul RHF76-052, ktorý sa ovládal pomocou AT príkazov. Toto koncové zariadenie bezdrôtovo komunikovalo so zostrojenou bránou z Raspberry Pi a koncentrátoru iC880A, ktorá dáta posielala na LoRa server bežiaci na tom istom zariadení. Server prijímal správy z brány a spracovával ich.

Po zostrojení siete boli podľa navrhnutých scenárov nasimulované bezpečnostné incidenty, ktoré v sieti spôsobovali DoS. Po úspešnej simulácii útokov boli navrhnuté možnosti detekcie na základe anomálií v sieti a graficky boli predvedené.

Literatúra

[1] MEKKI, K, E BAJIC, F CHAXEL a F MEYER. A comparative study of LPWAN technologies for large-scale IoT deployment. *Science Direct* [online]. [cit. 2020-06-08]. Dostupné z: https://www.sciencedirect.com/science/article/pii/S2405959517302953#fig1.

[2] LORA ALLIANCE. *What is LoRaWAN* [online]. [cit. 2020-06-08]. Dostupné z: https://lora-alliance.org/sites/default/files/2018-04/what-is-lorawan.pdf

[3] Internet of things (IoT). *IoT Agenda* [online]. [cit. 2020-06-08]. Dostupné z: https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT#targetText=The/20internet/20of/20things/2C/20or,human/2Dto/2Dcomputer/20interaction.

[4] GEMALTO, ACTILITY a SEMTECH. *LoRaWAN Security* [online]. 2017 [cit. 2020-06-08]. Dostupné z: https://lora-alliance.org/sites/default/files/2019-05/lorawan_security_whitepaper.pdf

[5] YANG, Xueying. *LoRaWAN: Vulnerability Analysis and Practical Exploitation* [online]. 2017 [cit. 2020-06-08]. Dostupné z: https://projets-ima.plil.fr/mediawiki/images/0/05/Thesis_Xueying_P27.pdf Delft University of Technology.

[6] Sensors – The Lifeblood of the Internet of Things. *Semielectronics* [online]. [cit. 2020-06-08]. Dostupné z: https://semielectronics.com/sensors-lifeblood-internet-things/

[7] *IoT Standards and Protocols* [online]. 2019 [cit. 2020-06-08]. Dostupné z: https://www.postscapes.com/internet-of-things-protocols

[8] *Open Standards Reference Model* Postcapes [online]. 2019 [cit. 2020-06-08]. Dostupné z: https://www.postscapes.com/wp-content/uploads/2018/03/unnamed-1-11.jpg

[9] Chirp spread spectrum. *Wikipedia* [online]. [cit. 2020-06-08]. Dostupné z: https://en.wikipedia.org/wiki/Chirp_spread_spectrum

[10] *Your Primer for LoRa/LoRaWAN* Medium [online]. 2018 [cit. 2020-06-08]. Dostupné z: https://medium.com/iotforall/your-primer-for-lora-lorawan-33f1e0eb4215

[11] N. SORNIN, M. LUIS, T. EIRICH, T. KRAMP a O. HERSENT. *LoRaWAN Specification v1.0.2* [online]. 2016 [cit. 2020-06-08]. Dostupné z: https://lora-alliance.org/sites/default/files/2018-05/lorawan1_0_2-20161012_1398_1.pdf

[12] N. SORNIN a A. YEGIN. *LoRaWAN Specification v1.1* [online]. 2017 [cit. 2020-06-08]. Dostupné z: https://lora-alliance.org/sites/default/files/2018-04/lorawantm_specification_-v1.1.pdf

[13] N. SORNIN a A. YEGIN. *LoRaWAN Backend Interfaces 1.0 Specification* [online]. 2017 [cit. 2020-06-08]. Dostupné z: https://lora-alliance.org/sites/default/files/2018-04/lorawantm-backend-interfaces-v1.0.pdf

[14] *National Institute of Standards and technology* [online]. [cit. 2020-06-08]. Dostupné z: https://www.nist.gov/

[15] *Backbone network* [online]. [cit. 2020-06-08]. Dostupné z: https://en.m.wikipedia.org/wiki/Backbone_network

[16] BUTUN, Ismail, Nuno PEREIRA a Mikael GIDLUND. *Analysis of LoRaWAN v1.1 security* [online]. 2018 [cit. 2020-06-08]. Dostupné z: http://delivery.acm.org/10.1145/3220000/3213304/a5-butun.pdf

[17] *Loriot* [online]. [cit. 2020-06-08]. Dostupné z: https://www.loriot.io

[18] Ai-Thinker *RHF-DS01500* RHF76-052 LoRaWAN Module Datasheet [online]. [cit. 2020-06-08]. Dostupné z: https://files.seeedstudio.com/wiki/Seeeduino_LoRa/res/rhf-ds01500_rhf76-052_datasheet_v03.pdf

[19] Microchip *RN2483* Low-Power Long Range LoRa Technology Transceiver Module [online]. [cit. 2020-06-08]. Dostupné z: https://www.alldatasheet.com/datasheet-pdf/pdf/792917/MICROCHIP/RN2483.html

[20] ESES *CP2102 USB TTL prevodník* [online]. [cit. 2020-06-08]. Dostupné z: https://arduino-shop.cz/docs/produkty/0/747/eses1449940303.pdf

[21] *Raspberry Pi* [online]. [cit. 2020-06-08]. Dostupné z: https://www.raspberrypi.org

[22] *Concentrator iC880A* [online]. [cit. 2020-06-08]. Dostupné z: https://wireless-solutions.de/products/long-range-radio/ic880a.html

[23] Serial Periphetal Interface *Wikipedia* [online]. [cit. 2020-06-08]. Dostupné z: https://en.wikipedia.org/wiki/Serial_Peripheral_Interface

[24] *IC880A-SPI QuickStart Guide* [online]. [cit. 2020-06-08]. Dostupné z: https://wireless-solutions.de/downloads/Radio-Modules/iC880A/iC880A-SPI_QuickStartGuide.pdf

[25] *Chirpstack* [online]. [cit. 2020-06-08]. Dostupné z: https://www.chirpstack.io/

[26] *Ubuntu MATE* [online]. [cit. 2020-06-08]. Dostupné z: https://ubuntu-mate.org

[27] *Hercules SETUP Utility* [online]. [cit. 2020-06-08]. Dostupné z: https://www.hw-group.com/software/hercules-setup-utility

[28] *Arduino IDE* [online]. [cit. 2020-06-08]. Dostupné z: https://www.arduino.cc/en/main/software

[29] DANISH, Syed Muhammad, Arfa NASIR, Hassaan Khaliq QURESHI, Ayesha Binte ASHFAQ, Shahid MUMTAZ a Jonathan RODRIGUEZ. *Network Intrusion Detection System for Jamming Attack in LoRaWAN join procedure* [online]. National University of Science & Technology [cit. 2020-06-08]. Dostupné z: https://www.researchgate.net/publication/327123739_Network_Intrusion_Detection_System_for_Jamming_Attack_in_LoRaWAN_Join_Procedure

[30] Hamming distance *Wikipedia* [online]. [cit. 2020-06-08]. Dostupné z: https://en.wikipedia.org/wiki/Hamming_distance

[31] *Wireshark* [online]. [cit. 2020-06-08]. Dostupné z: https://www.wireshark.org/

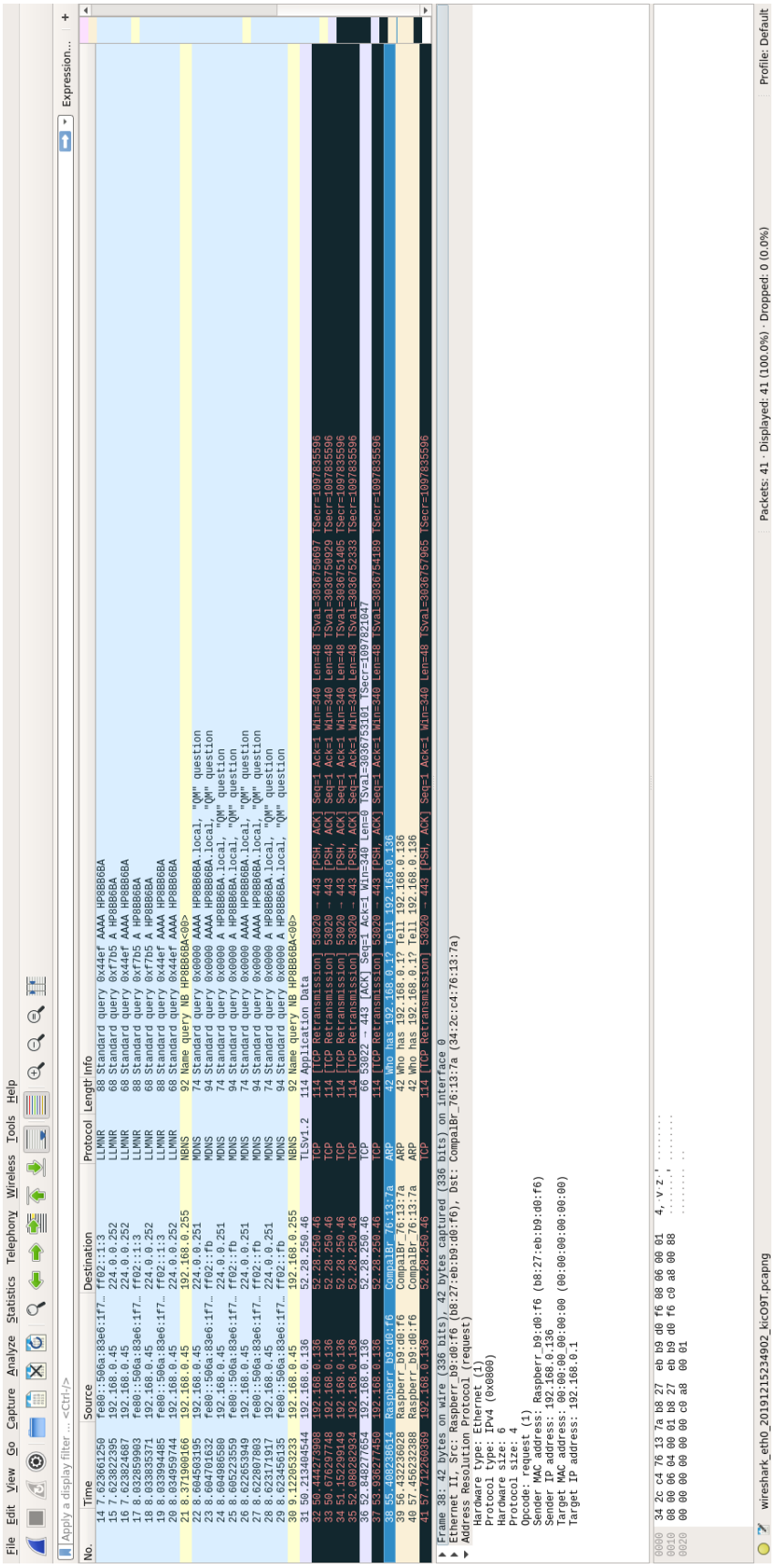
Zoznam symbolov, veličín a skratiek

3GPP	3rd Generation Partnership Project
ABP	Activation By Personalization
ACK	Acknowledgment
ADR	Adaptive Data Rate
AES	Advanced Encryption Standard
AppKey	Application Key
AppSKey	Application Session Key
AT	Attention These
B	Byte (Bajt)
b	bit
BPSK	Binary Phase Shift Keying
CMAC	Cipher-based Message Authentification Code
CoAP	Constrained Application Protocol
CSS	Chirp Spread Spectrum
CTR	Counter Mode Encryption
dB	Decibel
DevAddr	Device Address
DoS	Denial of Service
DTLS	Datagram Transport Layer
FDMA	Frequency Division Multiple Access
FNwkSEncKey	Forwarding Network Session Encryption Key
FSK	Frequency Shifting Keying
Gb	Gigabit
GHz	Gigahertz
GPRS	General Packet Radio Service
GSM	Global Systems for Mobile communications
HTTP	Hyper Text Transport Protocol
HTTPS	Hyper Text Transport Protocol Secure
Hz	Hertz
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
IP	Internet Protocol
IPv6	Internet Protocol version 6
ISO	International Organization for Standardization
kb	Kilobit
LoRaWAN	Long Range Wide Area Network

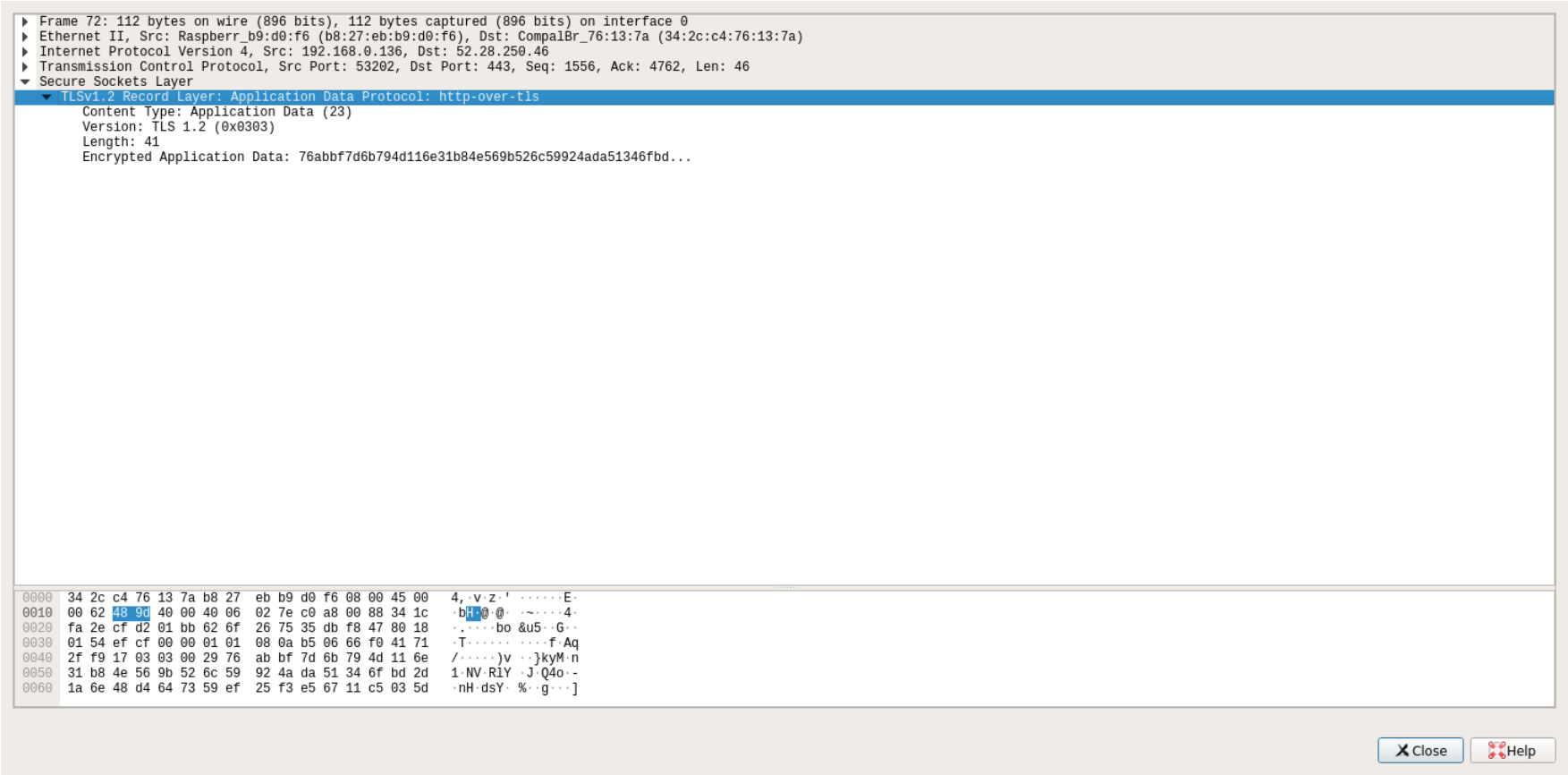
LoWPAN Low Power Wireless Personal Area Network
LPWAN Low Power Wide Area Network
LSB Least Significant Bit
LTE Long Term Evolution
LWM2M Lightweight Machine to Machine
MAC Media Access Control
Mb Megabit
MHz Megahertz
MIC Message Integrity Code
MITM Man In The Middle
MQTT Message Queuing Telemetry Transport
NB-IoT NarrowBand Internet of Things
NFC Near Field Communication
NIST National Institute of Standards and Technology
NVRAM Non-Volatile Random Access Memory
NwkKey Network Key
NwkSEncKey Network Session Encryption Key
NwkSKey Network Session Key
OSI Open Systems Interconnection
OTAA Over The Air Activation
OTrP Open Trust Protocol
QoS Quality of Service
QPSK Quadrature Phase-Shift Keying
SF Spread Factor
SNwkSIncKey Serving Network Session Intergrity Key
SPI Serial Peripheral Interface
SSI Simple Sensor Interface
TCP Transmission Control Protocol
TEE Trusted Execution Enviroment
TLS Transport Layer Security
TSMP Time Synchronized Mesh Protocol
UDP User Datagram Protocol
VPN Virtual Private Network
XML Extensible Markup Language
XMPP Extensible Messaging and Presence Protocol

Zoznam príloh

A Zachytené pakety z brány



Obr. A.1: Pakety zachytené na bráne pri výpadku siete.



Obr. A.2: Zachytený paket s aplikačnými dátami.

B Obsah priloženého CD

- `/` ..... koreňový adresár priloženého CD
  - `Zdrojové kódy` ..... Zdrojové kódy
    - `jammer.ino` ..... Zdrojový kód jammera
    - `parser.py` ..... Zdrojový kód detekčného programu
  - `Bakalárska práca.pdf` ..... Bakalárska práca v elektronickej podobe